

# Contents

[Cloud Adoption Framework for Azure](#)

[About the Framework](#)

[What's new](#)

[Get started](#)

[Overview](#)

[Foundational alignment](#)

[Document foundational alignment decisions](#)

[How does Azure work?](#)

[Azure fundamental concepts](#)

[Portfolio hierarchy](#)

[Azure hierarchy support](#)

[Accelerate adoption](#)

[Accelerate migration](#)

[Build new products and services](#)

[Unblock environment design and configuration](#)

[Improve controls](#)

[Enable customer success](#)

[Deliver operational excellence](#)

[Manage cloud costs](#)

[Secure the enterprise environment](#)

[Improve reliability](#)

[Ensure consistent performance](#)

[Establish teams](#)

[Align your organization](#)

[Build a cloud strategy team](#)

[Build a cloud adoption team](#)

[Build a cloud governance team](#)

[Build a cloud operations team](#)

[Strategy](#)

Overview

Motivations

Business outcomes

Overview

Data innovation

Data democratization

Fiscal outcomes

Agility outcomes

Global reach outcomes

Customer engagement outcomes

Performance outcomes

Sustainability outcomes

Business outcome template

Align efforts to learning metrics

Objectives and key results

Business justification

Build a business justification

Create a financial model

Understand cloud accounting

Align your partner strategy

First cloud adoption project

Additional considerations

Balance competing priorities

Balance the portfolio

Global markets

Define security strategy

Define monitoring strategy

Responsible AI

Skills relevant to strategy

Plan

Overview

Digital estate

The five Rs of rationalization

## THE FIVE Rs OF RATIONALIZATION

What is a digital estate?

Digital estate planning

Gather inventory data

Rationalize the digital estate

Align cost models to forecast costs

Measure business outcomes with AppDynamics

Initial organization alignment

Skills readiness plan

Build a readiness plan

Map roles and skills

Cloud adoption plan

Overview

Prerequisites

Deploy the template to Azure DevOps

Define and prioritize workloads

Align assets to workloads

Review rationalization decisions

Establish iterations and release plans

Estimate timelines

Best practices

Digital estate assessment in Azure

Plan a data warehouse migration

Ready

Overview

Azure setup guide

Setup guide overview

Organize resources

Manage access

Manage costs and billing

Plan governance, security, and compliance

Establish monitoring and reporting

Stay current with Azure

## Operating model

Overview

Define your operating model

Compare common cloud operating models

Common operating model terms

## Azure landing zones

What is a landing zone?

Design areas

Implementation options

Start with enterprise scale

Overview

Implement enterprise-scale landing zones

Architecture

Design principles

Design guidelines

Critical design areas

Enterprise enrollment and Azure AD tenants

Identity and access management

Management group and subscription organization

Network topology and connectivity

Management and monitoring

Business continuity and disaster recovery

Security, governance, and compliance

Platform automation and DevOps

Implementation guidelines

Transition to enterprise-scale (brownfield)

Start small and expand

CAF Migration landing zone blueprint

CAF Foundation blueprint

Terraform landing zones

Expand your landing zone

Basic landing zone considerations

## Overview

- Review compute options
- Review networking options
- Review storage options
- Review data options
- Role-based access control
- Create hybrid cloud consistency
- Improve landing zone operations
- Improve landing zone governance
- Improve landing zone security

## Overview

- Onboard a subscription to Azure Security Center
- Onboard Azure Sentinel
- Implementing a secure hybrid network architecture in Azure
- Azure identity management and access control security best practices
- Azure network security best practices
- Azure operational security best practices

Partner landing zones

Infrastructure-as-code theory

- Refactor landing zones
- Test-driven development (TDD) for landing zones
- Landing zone TDD in Azure

Best practices

## Overview

Resource organization

- Create your initial subscriptions
- Scale with multiple subscriptions
- Organize your subscriptions
- Naming and tagging
- Move resources

Networking

- Network boundary security

- Plan virtual networks
  - Best practices for network security
  - Perimeter networks
  - Hub and spoke network topology
- Identity and access controls
  - Identity management best practices
  - Secure privileged access
  - Choose an authentication method
- Storage
  - Storage security guide
- Databases
  - Database security best practices
  - Choose a deployment option in Azure SQL
- Cost management
  - Track costs
  - Optimize your cloud investment
  - Create and manage budgets
  - Export cost data
  - Optimize costs from recommendations
  - Monitor usage and spending
- Skills relevant to ready and landing zones
- Adopt
  - Migrate
    - Overview
    - Azure migration guide
      - Migration guide overview
      - Assess workloads
      - Deploy workloads
      - Release workloads
      - Migration-focused cost-control mechanisms
      - Get assistance
    - Migration scenarios

## [Overview](#)

[Contoso overview](#)

[Windows Server workloads](#)

[Rehost a Windows app on Azure VMs](#)

[SQL Server workloads](#)

[Migrate SQL Server databases to Azure](#)

[Rehost an app on Azure VMs and Azure SQL Managed Instance](#)

[Rehost an app on Azure VMs and SQL Server Always On availability groups](#)

[Linux and open-source databases](#)

[Migrate open source databases to Azure](#)

[Migrate MySQL to Azure](#)

[Migrate PostgreSQL to Azure](#)

[Migrate MariaDB to Azure](#)

[Rehost a Linux app on Azure VMs](#)

[Rehost a Linux app on Azure VMs and Azure Database for MySQL](#)

[Dev/test workloads](#)

[Migrate dev/test environments to Azure IaaS](#)

[Migrate to Azure DevTest Labs](#)

[ASP.NET and PHP web apps](#)

[Refactor a Windows app onto App Service and Azure SQL Database](#)

[Refactor a Windows app onto App Service and SQL Managed Instance](#)

[Refactor a Linux app onto App Service and MySQL](#)

[Rebuild an app in Azure](#)

[Refactor TFS to Azure DevOps Services](#)

[Java apps](#)

[Migration overview](#)

[Spring to Azure App Service](#)

[Tomcat to Azure App Service](#)

[Tomcat to containers on AKS](#)

[WebLogic to Azure Virtual Machines](#)

[WildFly to WildFly on AKS](#)

[WebLogic to WildFly on AKS](#)

[WebSphere to WildFly on AKS](#)

[JBoss EAP to WildFly on AKS](#)

SAP

[SAP migration guide](#)

[Migrate SAP applications to Azure](#)

[Migration methodologies for SAP on Azure](#)

Specialized workloads

[Move on-premises VMware infrastructure to Azure](#)

[Azure NetApp Files](#)

[Oracle in Azure](#)

[Cray in Azure](#)

[VDI](#)

VMware hosts

[Considerations when rehosting VMware](#)

Prerequisites

[Secure your environment](#)

[Private cloud management](#)

[Private cloud networking](#)

[VMware platform](#)

[Azure core integration](#)

Rehost and disaster recovery options

[Rehost workload VMs to Private Cloud vCenter](#)

[Rehost data using Azure Data Box](#)

[Back up workload VMs](#)

[Set up CloudSimple Private Cloud as disaster recovery site using Zerto](#)

[Set up CloudSimple Private Cloud as disaster recovery site using VMware SRM](#)

Windows Virtual Desktop

[Overview](#)

[Planning](#)

[Azure landing zone review](#)

[Proof of concept](#)

[Assess](#)

[Migrate \(or Deploy\)](#)

[Release](#)

[Data platforms](#)

[Overview](#)

[Azure Database Migration Guide](#)

[Refactor SQL Server to Azure SQL Database](#)

[Refactor SQL Server to Azure SQL Managed Instance](#)

[Refactor SQL Server to SQL Server on Azure VMs](#)

[Refactor SQL Server to Azure SQL Data Warehouse](#)

[MySQL](#)

[PostgreSQL](#)

[MariaDB](#)

[MongoDB](#)

[Cassandra](#)

[Oracle](#)

[DB2](#)

[SAP ASE](#)

[Access](#)

[Azure Database Migration Service \(DMS\) tutorials](#)

[Azure Database Migration Service overview](#)

[Migrate SQL Server to Azure SQL Database offline](#)

[Migrate SQL Server to Azure SQL Database online](#)

[Migrate SQL Server to Azure SQL Managed Instance offline](#)

[Migrate SQL Server to Azure SQL Managed Instance online](#)

[Migrate Amazon RDS SQL Server to Azure SQL Database or Azure SQL Managed Instance online](#)

[Migrate MySQL to Azure Database for MySQL online](#)

[Migrate Amazon RDS MySQL to Azure Database for MySQL online](#)

[Migrate PostgreSQL to Azure Database for PostgreSQL online](#)

[Migrate Amazon RDS PostgreSQL to Azure Database for PostgreSQL online](#)

[Migrate MongoDB to Azure Cosmos DB's API for MongoDB offline](#)

[Migrate MongoDB to Azure Cosmos DB's API for MongoDB online](#)

[Migrate Oracle to Azure Database for PostgreSQL online](#)

## Azure Stack

[Overview](#)

[Planning](#)

[Azure landing zone review](#)

[Assess](#)

[Migrate \(or Deploy\)](#)

[Govern](#)

[Manage](#)

## Analytics solutions

[Overview](#)

[Teradata](#)

[Netezza](#)

[Exadata](#)

## Mainframes

[Overview](#)

[Myths and facts](#)

[Switch from mainframes to Azure](#)

[Mainframe application migration](#)

## Migrate secure workloads

[Securing and managing workloads after migration](#)

[Azure database security best practices](#)

[Azure data security and encryption best practices](#)

[Azure PaaS best practices](#)

[Azure Service Fabric security best practices](#)

[Best practices for Azure VM security](#)

[IoT security best practices](#)

[Securing PaaS databases in Azure](#)

[Securing PaaS web and mobile applications using Azure App Service](#)

[Securing PaaS web and mobile applications using Azure Storage](#)

[Security best practices for IaaS workloads in Azure](#)

## Best practices

[Overview](#)

Multiple datacenters

Multiple regions

Data requirements exceed network capacity

Set up networking for migrated workloads

Deploy a migration infrastructure

Cost optimize migrated workloads

Scale a migration

Schema migration Data Definition Languages

High availability for Azure Synapse

Governance or compliance

Process improvements

Overview

Prerequisites

Overview

Decisions that affect migration

Environment planning checklist

Align roles and responsibilities

Agile change management

Migration backlog review

Assess workloads

Validate assessment assumptions before migration

Classify workloads

Keep priorities aligned

Evaluate workload readiness

Architect workloads

Update and refine initial cloud estimates

Understand partnership options

Manage change

Approve architecture changes

Deploy workloads

Overview

Promotion models

- Remediate assets
  - Replicate assets
  - Replicate options
  - Stage workloads
  - Release workloads
  - Overview
  - Business change plan
  - Business testing
  - Benchmark and resize assets
  - Prepare for promotion
  - Promote to production
  - Decommission retired assets
  - Conduct retrospectives
  - Skills relevant to migrate
- Innovate
- Overview
  - Azure innovation guide
    - Innovation guide overview
    - Prepare for customer feedback
    - Democratize data
    - Engage customers through apps
    - Empower adoption
    - Interact through devices
    - Innovate with AI
  - Innovation scenarios
    - Kubernetes
      - Innovation with Kubernetes
      - Application development and deployment
      - Cluster design and operations
      - Cluster and application security
    - Artificial intelligence (AI)
      - Innovate with AI

- Machine learning
- AI apps and agents
- Knowledge mining
- Best practices
  - Overview and Azure toolchain
  - Democratize data
    - Overview
    - Share data with experts
      - Quickly generate data insights
      - Sharing data with coworkers and partners
      - Embed reports in a website or portal
      - Create new workspaces in Power BI
    - Govern data
      - Classify data
      - Secure data
      - Annotate data with Data Catalog
      - Document data sources with Data Catalog
    - Centralize data
      - Create and query an Azure Synapse Analytics SQL pool
      - Best practices for loading data for data warehousing
      - Visualize warehouse data with Power BI
      - Reference architecture for enterprise BI with Azure Synapse Analytics
      - Manage enterprise big data with Azure Data Lake Storage
      - What is a data lake?
    - Collect data
      - Migrate on-premises data to Azure from SQL, Oracle, or NoSQL platforms
      - Integrate cloud data sources with a SQL Analytics data warehouse
      - Load on-premises data into Azure Synapse Analytics
      - Integrate data - Azure Data Factory to OLAP
      - Use Azure Stream Analytics with Azure Synapse Analytics
      - Reference architecture for ingestion and analysis of new feeds
      - Load data into Azure Synapse Analytics SQL pool

## Engage via apps

Overview

Citizen developers

PowerApps overview

Creating apps in PowerApps

Create your first workflow with Power Automate

Using AI Builder

Compliance and data privacy for citizen developer solutions

Data loss prevention policies for citizen developer solutions

Intelligent experiences

Modern web apps

Infusing intelligence

Chatbots

Cloud-native applications

Microservices architecture

Containers

Spring Boot microservices

Event-driven applications

Empower adoption

Overview

Shared solution

Get started with a shared repository - GitHub and Git

Get started with a shared backlog

Synchronize PowerApps with Azure DevOps

Feedback loops

Manage feedback with Azure DevOps

Continuous integration

Continuous integration with Azure Pipelines and GitHub

MLOps with Azure Machine Learning

Reliable testing

Manage and track test plans

Solution deployment

## Continuous deployment with Azure Pipelines and GitHub

### Integrated metrics

[Monitor ASP.NET applications](#)

[Monitor ASP.NET Core web applications](#)

[Monitor Node.js applications](#)

[Monitor mobile applications](#)

[Monitor web applications](#)

[Monitor VMs hosting traditional applications](#)

### Interact with devices

#### Overview

#### Mobile experience

[Extend a legacy claims-processing app with a web and mobile experience](#)

[Optimize reports to share data on a mobile app](#)

[Extend PowerApps canvas app to a mobile experience](#)

[Extend Power Automate to add a mobile experience](#)

[Secure mobile experiences](#)

#### Mixed reality

[Develop mixed reality experiences with Unity](#)

[Quickstarts to add Azure Spatial Anchors to a mixed reality solution](#)

### Integrated reality and IoT

[Visualize sensor data with Azure IoT in Power BI](#)

[Visualize sensor data with Azure IoT Hub in a web solution](#)

[Securing an IoT solution](#)

[Get started with Azure Sphere](#)

[Create a deployment with Azure Sphere](#)

[Get started with Azure Kinect DK](#)

[Build your first Azure Kinect DK app](#)

### Adjusted reality

[Azure Digital Twins + HoloLens: Adjusting virtual reality](#)

[Get started with Azure Digital Twins](#)

[Monitor a building with Azure Digital Twins](#)

[Azure IoT for cloud-to-device communications guide](#)

## Azure IoT configuration for cloud-to-device communications

### Innovate with AI

Overview

Machine learning

What is Machine Learning

Azure Machine Learning workflow

Analyze data with Azure Machine Learning

Deploy predictions

AI apps and agents

What are AI apps

What are AI agents

Knowledge mining

What is Azure Cognitive search

### Process improvements

Overview

Business value consensus

Customer adoption

Feedback loops

Build with customer empathy

Measure for customer impact

Learn with customers

Customer challenges and blockers

Digital invention

Develop digital inventions

Democratize data

Engage via apps

Empower adoption

Interact with devices

Predict and influence

### Govern

Overview

Methodology

## Benchmark

Initial governance foundation

Governance foundation improvements

Governance guides

Overview

Standard enterprise governance guide

Overview

Narrative

Initial corporate policy

Prescriptive guidance

Improve the Security Baseline discipline

Improve the Resource Consistency discipline

Improve the Cost Management discipline

Multicloud scenarios

Governance guide for complex enterprises

Overview

Narrative

Initial corporate policy

Prescriptive guidance

Improve the Identity Baseline discipline

Improve the Security Baseline discipline

Improve the Resource Consistency discipline

Improve the Cost Management discipline

Multicloud scenarios

Multiple layers of governance

Governance considerations

Evaluate corporate policy

Cloud-ready corporate policy and compliance

Make corporate policy cloud-ready

Understand business risks

Evaluate risk tolerance

Define corporate policy

- [Align design with policy](#)
- [Establish policy adherence processes](#)
- [Regulatory compliance](#)
- [Cloud security readiness](#)
- [Cloud policy review](#)
- [Data classification](#)
- [Disciplines of cloud governance](#)
- [Implement disciplines of cloud governance](#)
- [Cost management](#)
  - [Overview of cost management](#)
  - [Download the template](#)
  - [Understand business risks](#)
  - [Risk tolerance metrics and indicators](#)
  - [Sample Cost Management policies](#)
  - [Policy compliance processes](#)
  - [Improve cost management](#)
  - [Best practices](#)
  - [Azure tools for cost management](#)
- [Security baseline](#)
  - [Overview of the security baseline](#)
  - [Download the template](#)
  - [Understand business risks](#)
  - [Risk tolerance metrics and indicators](#)
  - [Sample Security Baseline policies](#)
  - [Policy compliance processes](#)
  - [Improve the security baseline](#)
  - [Cloud-native security baseline](#)
  - [Additional Azure security guidance](#)
  - [Azure tools for security baseline](#)
- [Identity baseline](#)
  - [Overview of the identity baseline](#)
  - [Download the template](#)

- Understand business risks
  - Risk tolerance metrics and indicators
  - Sample Identity Baseline policies
  - Policy compliance processes
  - Improve the identity baseline
  - Azure tools for identity baseline
- Resource consistency
  - Overview of resource consistency
  - Download the template
  - Understand business risks
  - Risk tolerance metrics and indicators
  - Sample Resource Consistency policies
  - Policy compliance processes
  - Improve resource consistency
  - Azure tools for resource consistency
  - Resource access management
  - Governance design for a simple workload
  - Governance design for multiple teams
- Deployment acceleration
  - Deployment acceleration
  - Overview of deployment acceleration
  - Download the template
  - Understand business risks
  - Risk tolerance metrics and indicators
  - Sample Deployment Acceleration policies
  - Policy compliance processes
  - Improve deployment acceleration
  - Azure tools for deployment acceleration
- Manage
  - Overview
  - Azure management guide
  - Before you start
  - Inventory and visibility

Operational compliance

Protect and recover

Enhanced baseline

Platform specialization

Workload specialization

Best practices

Overview

Azure server management services

Introduction to Azure server management services

Getting ready for cloud operations

Get started with cloud operations

Overview

Configure the service for a single VM

Configure the service for an entire subscription

Configure at scale with automation

Set up basic alerts

Ongoing cloud operations

Overview

Enable guest configuration policy

Critical changes (tracking and alerting)

Update schedules

Common policies in Azure

Review of tools and services

Monitoring

Overview

Monitoring cloud models

Data collection

Alerting

Monitoring platforms overview

Skills relevant to monitoring

Centralize management operations

Establish an operational fitness review

Improving platform or workload reliability

Reliability checklist for Azure services

Failure mode analysis

Recover from a region wide service disruption

Recover from data corruption or accidental deletion

Management considerations

Overview

Business alignment

Define criticality

Understand business impact

Establish business commitments

Management disciplines

Inventory and visibility

Operational compliance

Protect and recovery

Platform operations

Workload operations

Advanced management and system design

Organize

Managing organization alignment

Required cloud functions

Cloud strategy functions

Cloud adoption functions

Cloud governance functions

Central IT functions

Cloud operations functions

Cloud center of excellence functions

Cloud platform functions

Cloud automation functions

Cloud data functions

Cloud security functions

Cloud security team functions

- Policy and standards
- Security operations center (SOC)
- Security architecture
- Security compliance management
- People security
- Application security and DevSecOps
- Data security
- Infrastructure and endpoint security
- Identity and keys
- Threat intelligence
- Posture management
- Incident preparation

Mature teams structure

Align the RACI matrix

Building technical skills

Creating a cost-conscious organization

Anti-patterns - IT fiefdoms and IT silos

## Resources

- Tools and templates
- Azure security best practices
- Decision guides
  - Overview
  - Subscriptions
  - Identity
  - Policy enforcement
  - Resource consistency
  - Resource tagging
  - Encryption
- Software-defined networks
  - Overview
  - PaaS-only
  - Cloud-native

[Cloud DMZ](#)

[Hybrid](#)

[Hub and spoke model](#)

[Logging and reporting](#)

[Migration tools](#)

[Additional resources](#)

[Azure Architecture Center for solution architecture](#)

[Microsoft Azure Well-Architected Framework for workload architecture](#)

[Docs for product implementation](#)

[Learn to develop skills](#)

[Assessments to personalize guidance](#)

[Archived resources](#)

[Cloud Operating Model](#)

[Azure enterprise scaffold](#)

[Virtual Datacenter \(VDC\)](#)

# What is the Microsoft Cloud Adoption Framework for Azure?

11/9/2020 • 3 minutes to read • [Edit Online](#)

The Microsoft Cloud Adoption Framework for Azure is proven guidance that's designed to help you create and implement the business and technology strategies necessary for your organization to succeed in the cloud. It provides best practices, documentation, and tools that cloud architects, IT professionals, and business decision makers need to successfully achieve short-term and long-term objectives.

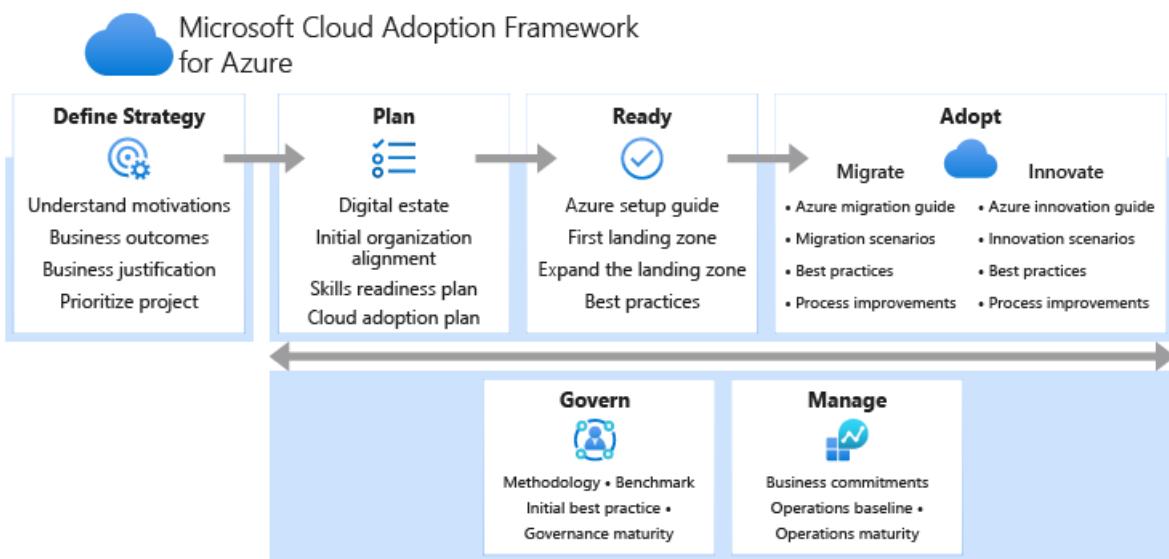
By using the Microsoft Cloud Adoption Framework for Azure best practices, organizations can better align their business and technical strategies to ensure success. Watch the following video to learn more.

The Cloud Adoption Framework brings together cloud adoption best practices from Microsoft employees, partners, and customers. It provides a set of tools, guidance, and narratives that help shape technology, business, and people strategies for driving desired business outcomes during your cloud adoption effort. Review the guidance for each methodology below, providing you with easy access to the right guidance at the right time.

	<b>Strategy:</b> define business justification and expected outcomes of adoption.		<b>Plan:</b> align actionable adoption plans to business outcomes.
	<b>Ready:</b> Prepare the cloud environment for the planned changes.		<b>Migrate:</b> Migrate and modernize existing workloads.
	<b>Innovate:</b> Develop new cloud-native or hybrid solutions.		<b>Govern:</b> Govern the environment and workloads.
	<b>Manage:</b> Operations management for cloud and hybrid solutions.		<b>Organize:</b> Govern the environment and workloads.

## Understand the lifecycle

Each methodology above is part of a broad cloud adoption lifecycle. The Cloud Adoption Framework is a full lifecycle framework, supporting customers throughout each phase of adoption by providing methodologies as specific approaches to overcoming common blockers, as shown here.



## Intent

The cloud fundamentally changes how enterprises procure, use, and secure technology resources. Traditionally, enterprises assumed ownership of and responsibility for all aspects of technology, from infrastructure to software. By moving to the cloud, enterprises can provision and consume resources only when they're needed. Although the cloud offers tremendous flexibility in design choices, enterprises need a proven and consistent methodology for adopting cloud technologies. The Microsoft Cloud Adoption Framework for Azure meets that need, helping guide decisions throughout cloud adoption.

But cloud adoption is only a means to an end. Successful cloud adoption starts well before a cloud platform vendor is selected. It begins when business and IT decision makers realize that the cloud can accelerate a specific business transformation objective. The Cloud Adoption Framework helps align strategies for business, culture, and technical change to achieve their desired business outcomes.

The Cloud Adoption Framework provides technical guidance for Microsoft Azure. Because enterprise customers might still be in the process of choosing a cloud vendor or might have an intentional multicloud strategy, the framework provides cloud-agnostic guidance for strategic decisions whenever possible.

## Intended audience

This guidance affects the business, technology, and culture of enterprises. The affected roles include line-of-business leaders, business decision makers, IT decision makers, finance, enterprise administrators, IT operations, IT security and compliance, IT governance, workload development owners, and workload operations owners. Each role uses its own vocabulary, and each has different objectives and key performance indicators. A single set of content can't address all audiences effectively.

Enter the *cloud architect*. The cloud architect serves as the thought leader and facilitator to bring these audiences together. We've designed this collection of guides to help cloud architects facilitate the right conversations with the right audiences and drive decision-making. Business transformation that's empowered by the cloud depends on the cloud architect role to help guide decisions throughout the business and IT.

Each section of the Cloud Adoption Framework represents a different specialization or variant of the cloud architect role. These sections also create opportunities to share cloud architecture responsibilities across a team of cloud architects. For example, the governance section is designed for cloud architects who have a passion for mitigating technical risks. Some cloud providers refer to these specialists as cloud custodians; we prefer the term *cloud guardian* or, collectively, the *cloud governance team*.

## How to use the Microsoft Cloud Adoption Framework for Azure

If your enterprise is new to Azure, begin by [understanding and documenting foundational alignment decisions](#). When your enterprise's digital transformation involves the cloud, understanding these fundamental concepts will help you during each step of the process.

[Get started](#)

# What's new in the Microsoft Cloud Adoption Framework for Azure

11/9/2020 • 13 minutes to read • [Edit Online](#)

Here's a list of recent changes made to the Cloud Adoption Framework.

This framework is built collaboratively with customers, partners, and internal Microsoft teams. New and updated content is released when it becomes available. These releases allow you to test, validate, and refine the guidance along with us. We encourage you to partner with us to build the Cloud Adoption Framework.

## October 2020

This month's updates include incremental improvements throughout the Cloud Adoption Framework and supporting web assets.

Our biggest investments have focused on building out Microsoft Learn modules to accelerate application of the Cloud Adoption Framework. This month, we released the modules listed below. Note that the Getting Started module provides our first guidance aligned with an industry vertical, by introducing a retail customer (Tailwind Traders) who we will follow through all of the core methodology modules to follow.

MODULE	DESCRIPTION
<a href="#">Overview module</a>	Entry-level introduction to the framework.
<a href="#">Getting Started module</a>	Introduction to the getting started guides to accelerate application of the proper methodologies for overcoming specific blockers.
<a href="#">Azure landing zones</a>	Before building out your cloud environment, understand your operating requirements and choose the most appropriate Azure landing zone product to get you started.
<a href="#">Create an enterprise-scale architecture</a>	Create landing zones at scale following a set of enterprise-scale design principles, reference architectures, and reference implementations. Four modules to create a single learning path to success.

We've also expanded the business outcomes to share a number of common business motivations and approaches that continue to emerge in the post-COVID marketplace.

ARTICLE	DESCRIPTION
<a href="#">Examples of sustainability outcomes</a>	Learn how cloud computing can help you reduce carbon emissions, use resources more efficiently, and shrink your environmental footprint.
<a href="#">Measure business outcomes with objectives and key results (OKRs)</a>	Learn how to use OKRs to measure business outcomes.

ARTICLE	DESCRIPTION
<a href="#">Measure business outcomes with AppDynamics</a>	Understanding an application's performance and user experience is key to measuring business outcomes. See how AppDynamics can provide business insights for most use cases.
<a href="#">Cost management update: Spot VMs</a>	Use of Spot VMs in nonproduction environments is a rapidly emerging practice to further reduce costs in those environments. "I already have a working environment. How can I apply the design principles of enterprise-scale?" The new article on transitioning to enterprise-scale can help.

ARTICLE	DESCRIPTION
<a href="#">Transition existing Azure environments to enterprise-scale</a>	This article helps organizations to navigate the right path based on an existing Azure environment transitioning into enterprise-scale.
<a href="#">Cloud Adoption Framework enterprise-scale landing zone architecture</a>	This article was updated to include a high-level diagram for an enterprise-scale landing zone architecture based on the hub and spoke network topology, and updates to describe and cross-reference the critical design areas for an enterprise-scale landing zone architecture.

## August 25, 2020

This release provides better definition and decision criteria regarding landing zone implementations.

### Operating model

One of the most important considerations in landing zone design and implementation is your operating model. How you want to operate in the cloud will have a direct impact on the architecture and controls to implement. The following articles will help align your target operating model with a few models that are common in the cloud. Then map those to the most appropriate implementation to get started.

ARTICLE	DESCRIPTION
<a href="#">Compare common operating models</a>	This article is the primary guide for comparing operating models and choosing a course of action.
<a href="#">Understand cloud operating models</a>	Primer for making import decisions regarding your operating model.
<a href="#">Define your operating model with CAF</a>	The Cloud Adoption Framework is an incremental guide to building out your environment and adopting the cloud within your chosen operating model. This article creates a frame of reference to understand how the various methodologies support the development of your operating model.
<a href="#">Terms</a>	Terms that are likely to come up when discussing your operating model with counterparts. These terms are not as commonly used by architects or technical specialists, but will prove important in those conversations.

### Azure landing zones: Additional implementation options

The concept and implementations options behind Azure landing zones was built alongside the leading Microsoft partners. This release recognizes the existing intellectual property (IP) that those partners use to accelerate cloud adoption.

ARTICLE	DESCRIPTION
<a href="#">Partner landing zones</a>	Review and compare Azure landing zone offers from your partner.
<a href="#">Implementation options</a>	Updated to add partner landing zone options to the existing Azure landing zone implementation options.
<a href="#">Enterprise-scale reference implementations</a>	Updated to add a hub-spoke reference implementation to enterprise-scale reference implementations.

#### NOTE

The new partner landing zone articles don't specify how a partner should define or implement a landing zone. Instead, it's designed to add structure to a complex conversation, so you can better understand the partner offer. This list of questions and minimum evaluation criteria can also be used to compare offers from potential partners. It's also being used by some partners to more clearly communicate the value of their Azure landing zone implementation options.

## July 17, 2020

This release adds a number of new scenarios to make cloud adoption more actionable.

#### Migration scenarios:

The new [migration scenarios overview page](#) builds on the Migrate methodology to demonstrate how Azure delivers on the "#OneMigrate" promise. It provides approaches to migrating multiple first and third-party scenarios to Azure. This includes three new migration scenarios:

ARTICLE	DESCRIPTION
<a href="#">Windows Virtual Desktop</a>	This scenario enables productivity boosts and accelerates the migration of various workloads to support the end-user experience.
<a href="#">Azure Stack</a>	Learn about deploying Azure in your datacenter using Azure Stack Hub.

#### Analytics in the Cloud Adoption Framework:

Analytics solutions are now included in the Microsoft Cloud Adoption Framework. These new topics highlight best practices for enabling analytics solutions during your cloud adoption journey.

ARTICLE	DESCRIPTION
<a href="#">Analytics solution for Teradata, Netezza, Exadata</a>	Learn about migrating legacy on-premises environments including Teradata, Netezza, and Exadata to modern analytics solutions.
<a href="#">High availability for Azure Synapse</a>	Learn about one of the key benefits of a modern cloud-based infrastructure, built-in high availability and disaster recovery.

ARTICLE	DESCRIPTION
<a href="#">Schema migration data definition languages (DDL)</a>	Learn about the database objects and associated processes when preparing to migrate existing data.

## AI in the Cloud Adoption Framework:

AI solutions and best practices are now integrated into the Microsoft Cloud Adoption Framework. These AI solutions can help accelerate innovation with predictions about customer's needs, automate business processes, discover information, find new ways to engage with customers, and deliver better experiences during your cloud adoption journey.

ARTICLE	DESCRIPTION
<a href="#">Responsible AI</a>	Learn about the AI principles you should consider when implementing AI solutions and learn how to establish a responsible AI strategy.
<a href="#">Azure innovation guide: Innovate with AI</a>	Learn about how you can innovate with AI and find the best solution based on your implementation needs.
<a href="#">AI in the Cloud Adoption Framework</a>	Review a prescriptive framework that includes the tools, programs, and content (best practices, configuration templates, and architecture guidance) to simplify adoption of AI and cloud-native practices at scale.
<a href="#">MLOps with Azure Machine Learning</a>	Learn about Machine Learning operations (MLOps) best practices.
<a href="#">Innovate with AI</a>	Learn about AI solutions (Machine Learning, AI applications and agents, knowledge mining) and best practices that can accelerate digital invention.

## June 15, 2020

Proper configuration of the cloud environment is often the first and most common technical blocker during cloud adoption. This release focuses heavily on guidance that accelerates deployment of cloud environments. To overcome this common blocker, the Cloud Adoption Framework introduces **Azure landing zones**.

ARTICLE	DESCRIPTION
<a href="#">Azure landing zones</a>	Azure landing zones create a common set of design areas and implementation options to accelerate environment creation aligned to the cloud adoption plan and cloud operating model. This new article defines Azure landing zones more clearly.
<a href="#">Azure landing zones: Design areas</a>	All Azure landing zones share a common set of 8 design areas. Before deploying any of the Azure landing zones, customers should consider each of these design to make critical decisions.
<a href="#">Azure landing zones: Implementation options</a>	Choose the best Azure landing zone implementation option, depending on your cloud adoption plan and cloud operating model.

The existing CAF blueprint definitions and CAF Terraform modules provide a starting point for Azure landing zone implementation. However, some customers need a richer implementation option that can meet the demands of

enterprise-scale cloud adoption plans. This release adds **CAF enterprise-scale** to the Azure landing zone implementation options to fill that need. The following lists a few of the articles to get you started with the CAF enterprise-scale architecture and reference implementations.

ARTICLE	DESCRIPTION
<a href="#">Enterprise-scale overview</a>	Overview to enterprise-scale
<a href="#">Implement CAF enterprise-scale landing zones</a>	Rapid implementation options and GitHub examples
<a href="#">Enterprise-scale architecture</a>	Understand the architecture behind enterprise-scale
<a href="#">Enterprise-scale design principles</a>	Understand the architectural design principles that guide decisions during implementation to evaluate whether this approach fits your cloud operating model
<a href="#">Enterprise-scale design guideline</a>	Evaluate the enterprise-scale guidelines for fulfilling the common design areas of Azure landing zones
<a href="#">Implementation guidelines</a>	Review the activities required for an enterprise-scale implementation before deployment

Partners are an important aspect of successful cloud adoption. Throughout the Cloud Adoption Framework guidance, we have added references to show the important role that partners play and how customers can better engage partners. For a list of validated CAF partners, see the [CAF-aligned partner offers](#), [Azure expert managed service providers \(MSPs\)](#), or [advanced specialist partners](#).

## May 15, 2020

Based on feedback, we've created new content to get you started using the Cloud Adoption Framework. The new getting started guides help you navigate the framework based on what you want to accomplish. We've also created a new landing page to make it easier to find the guidance, tools, learn modules and programs that support a successful cloud adoption journey.

ARTICLE	DESCRIPTION
<a href="#">Cloud Adoption Framework for Azure</a>	The Cloud Adoption Framework landing page has been redesigned to make it easier to find the guidance, tools, learn modules and programs that support a successful cloud adoption journey.
<a href="#">Get started with the Cloud Adoption Framework</a>	Choose a getting started guide that's aligned with your cloud adoption goals. These common scenarios provide a roadmap through the Microsoft Cloud Adoption Framework for Azure.
<a href="#">Understand and document foundational alignment decisions</a>	Learn about the initial decisions that every team involved in cloud adoption should understand.
<a href="#">Understand and align the portfolio hierarchy</a>	Learn how a portfolio hierarchy shows how your workloads and supporting services all fit together.
<a href="#">How do Azure products support the portfolio hierarchy?</a>	Learn about the Azure tools and solutions that support your portfolio hierarchy.

ARTICLE	DESCRIPTION
<a href="#">Manage organizational alignment</a>	Establish well-staffed organizational structures that an effective operating model for the cloud.

## April 14, 2020

We've brought all the cloud adoption tools and templates together in one place to make them easier to find.

ARTICLE	DESCRIPTION
<a href="#">Tools and templates</a>	Find the tools, templates, and assessments that can help you accelerate your cloud adoption journey.

## April 4, 2020

Continued iteration of refinement to the Migrate methodology and the Ready methodology, to more tightly align them with feedback from Microsoft customers, partners, and internal programs.

### Migrate methodology updates:

ARTICLE	DESCRIPTION
<a href="#">Migrate methodology</a>	These changes streamline the phases of the migration effort (assess workloads, deploy workloads, and release workloads). The changes also remove the details regarding the migration backlog. Removing those details and referencing plan, ready, and Adopt methodologies instead creates flexibility for various different cloud adoption programs to better align with the methodology.

### Ready methodology updates:

ARTICLE	DESCRIPTION
<a href="#">Refactor landing zones</a>	<b>New article:</b> Drawing from Ready methodology workshops, this article demonstrates the theory of starting with an initial template, using decision trees and refactoring to expand the landing zone, and moving toward a future state of enterprise readiness.
<a href="#">Expand your landing zone</a>	<b>New article:</b> Builds on the parallel iterations section of the refactoring article to show how various types of landing zone expansions would embed shared principles into the supporting platform. The original content for this overview has been moved to the <a href="#">basic landing zone considerations</a> node in the table of contents.
<a href="#">Test-driven development (TDD) for landing zones</a>	<b>New article:</b> The refactoring approach is much improved through the adoption of a test-driven development cycle to guide landing zone development and refactoring.
<a href="#">Landing zone TDD in Azure</a>	<b>New article:</b> Azure governance tools provide a rich platform for TDD cycles or red/green tests.

ARTICLE	DESCRIPTION
<a href="#">Improve landing zone security</a>	<b>New article:</b> Overview of the best practices in this section, related back to the TDD cycle.
<a href="#">Improve landing zone operations</a>	<b>New article:</b> List of best practices in the Manage methodology, with a transition to that modular approach to improving operations, reliability, and performance.
<a href="#">Improve landing zone governance</a>	<b>New article:</b> List of best practices related to Govern methodology, with a transition to that modular approach to improving governance, cost management, and scale.
<a href="#">Start with enterprise scale</a>	<b>New article:</b> Demonstrate an approach that shows the differences in the process, when a customer starts with CAF enterprise-scale landing zone templates. This article helps customers understand qualifiers that would support this decision.

## March 27, 2020

We've added guidance about the initial subscriptions you should create when you adopt Azure.

### Subscription guidance updates:

ARTICLE	DESCRIPTION
<a href="#">Create your initial Azure subscriptions</a>	<b>New article:</b> Create your initial production and nonproduction subscriptions, and decide whether to create sandbox subscriptions, as well as a subscription to contain shared services.
<a href="#">Create additional subscriptions to scale your Azure environment</a>	Learn about reasons to create additional subscriptions, moving resources between subscriptions, and tips for creating new subscriptions.
<a href="#">Organize and manage multiple Azure subscriptions</a>	Create a management group hierarchy to help organize, manage, and govern your Azure subscriptions.

## March 20, 2020

We've added prescriptive guidance that includes the tools, programs, and content categorized by persona to drive successful deployment of applications on Kubernetes, from proof of concept to production, followed by scaling and optimization.

### Kubernetes:

ARTICLE	DESCRIPTION
<a href="#">Application development and deployment</a>	<b>New article:</b> Provides checklists, resources, and best practices for planning application development, configuring CI/CD pipelines, and implementing site reliability engineering for Kubernetes.

ARTICLE	DESCRIPTION
<a href="#">Cluster design and operations</a>	<b>New article:</b> Provides checklists, resources, and best practices for cluster configuration, network design, future-proof scalability, business continuity, and disaster recovery for Kubernetes.
<a href="#">Cluster and application security</a>	<b>New article:</b> Provides checklists, resources, and best practices for Kubernetes security planning, production, and scaling.

## March 2, 2020

In response to feedback about continuity in the migration approach through multiple sections of the Cloud Adoption Framework, including Strategy, Plan, Ready, and Migrate, we've made the following updates. These updates are designed to make it easier for you to understand planning and adoption refinements as you continue a migration journey.

### Strategy methodology updates:

ARTICLE	DESCRIPTION
<a href="#">Balance the portfolio</a>	Moved this article to appear earlier in the Strategy methodology. This gives you visibility into the thought process earlier in the lifecycle.
<a href="#">Balancing competing priorities</a>	<b>New article:</b> Outlines the balance of priorities across methodologies to help inform your strategy.

### Plan methodology updates:

ARTICLE	DESCRIPTION
<a href="#">Assessment best practice</a>	Moved this article to the new "best practices" section of the Plan methodology. This gives you visibility into the practice of assessing local environments earlier in the lifecycle.

### Ready methodology updates:

ARTICLE	DESCRIPTION
<a href="#">What is a landing zone?</a>	<b>New article:</b> Defines the term landing zone.
<a href="#">First landing zone</a>	<b>New article:</b> Expands on the comparison of various landing zones.
<a href="#">CAF Migration landing zone</a>	Separated the blueprint definition from the selection of the first landing zone.
<a href="#">CAF Terraform modules</a>	Moved to the new "landing zone" section of the Ready methodology, to elevate Terraform in the landing zone conversation.

### Migrate methodology updates:

ARTICLE	DESCRIPTION
<a href="#">Overview</a>	Updated with a clearer description of the guide and fewer steps.
<a href="#">Assess</a>	Added a "challenging assumptions" section to demonstrate how this level of assessment works with the incremental assessment approach mentioned in the Plan methodology.
<a href="#">Classification during assess processes</a>	<b>New article:</b> Outlines the importance of classifying every asset and workload prior to migration.
<a href="#">Migrate</a>	Added a reference to UnifyCloud in the third-party tool options, in response to feedback at tier 1 conferences.
<a href="#">Test, optimize, and promote</a>	Aligned the title of this article with other process improvement suggestions.
<a href="#">Assess overview</a>	Updated to illustrate that the assessment in this phase focuses on assessing the technical fit of a specific workload and related assets.
<a href="#">Planning checklist</a>	Updated to clarify the importance of operations alignment during planning for migration efforts to ensure a well-managed workload following migration.

# Get started with the Cloud Adoption Framework

11/9/2020 • 2 minutes to read • [Edit Online](#)

The Cloud Adoption Framework can help you get started in several ways, so there are several different getting started guides. This article groups the guides to help you find the one that best aligns with your current challenges.

Each of the following links takes you to questions that are typically asked when an organization is trying to accomplish a certain goal during their cloud adoption journey.

- [Align foundational concepts to onboard a person, project, or team](#)
- [Adopt the cloud to deliver business and technical outcomes sooner](#)
- [Improve controls to ensure proper operations of the cloud](#)
- [Establish teams to support adoption and operations](#)

## Align foundation

A company's cloud adoption journey is typically built on a set of foundational decisions that impact the outcomes of a cloud adoption journey. The following information can help you make core decisions and record them as a reference to be used during the cloud adoption lifecycle.

- [Get started aligning foundation decisions](#)
- [How does Azure work](#)
- [Fundamental concepts](#)
- [Portfolio hierarchy](#)
- [Azure hierarchy support](#)

## Accelerate adoption

Cloud adoption requires technical change, but to digitally transform with the cloud, it requires more than just IT. Use these guides to start aligning various teams to accelerate migration and innovation efforts.

GUIDE	DESCRIPTION
<a href="#">We want to migrate existing workloads to the cloud.</a>	This guide is a great starting point if your primary focus is migrating on-premises workloads to the cloud.
<a href="#">We want to build new products and services in the cloud.</a>	This guide can help you prepare to deploy innovative solutions to the cloud.
<a href="#">We're blocked by environment design and configuration.</a>	This guide provides a quick approach to designing and configuring your environment.

## Improve controls

As your cloud adoption journey progresses, a solid operating model can help ensure that wise decisions are made. You'll also want to consider organizational change. These guides can help you align people and improve operations to develop your cloud operating model.

GUIDE	DESCRIPTION
<a href="#">How do we deliver operational excellence during cloud transformation?</a>	The steps in this guide can help the strategy team lead the organizational change management required to consistently ensure operational excellence.
<a href="#">How do we manage enterprise costs?</a>	This guide can help you start optimizing enterprise costs and manage cost across the environment.
<a href="#">How do we consistently secure the enterprise cloud environment?</a>	This guide can help ensure that the security requirements are applied across the enterprise to minimize risk of breach, and to accelerate recovery when a breach occurs.
<a href="#">How do we apply the right controls to improve reliability?</a>	This guide helps minimize disruptions related to inconsistencies in configuration, resource organization, security baselines, or resource protection policies.
<a href="#">How do we ensure performance across the enterprise?</a>	This guide can help you establish processes for maintaining performance across the enterprise.

## Establish teams

Depending on your adoption strategy and operating model, you might need to establish a few teams. This section helps you get those new teams started.

GUIDE	DESCRIPTION
<a href="#">How do we align our organization?</a>	This guide can help you establish an appropriately staffed organizational structure.
<a href="#">Do I need a cloud strategy team?</a>	This team ensures that cloud adoption efforts progress in alignment with business outcomes.
<a href="#">What does a cloud adoption team do?</a>	This team implements technical solutions outlined in the plan, and in accordance with governance requirements.
<a href="#">How do I build a cloud governance team?</a>	This team ensure that risks and risk tolerance are properly evaluated and managed.
<a href="#">How does a cloud operations team work?</a>	This team focuses on monitoring, repairing, and the remediation of issues related to traditional IT operations and assets.

# Get started: Understand and document foundational alignment decisions

11/9/2020 • 5 minutes to read • [Edit Online](#)

The cloud adoption journey can unlock many business, technical, and organizational benefits. Whatever you want to accomplish, if your journey involves the cloud, there are a few initial decisions that every team involved should understand.

## NOTE

Selecting any of the following links might lead you to bounce around the table of contents for the Microsoft Cloud Adoption Framework for Azure, looking for fundamental concepts that you'll use later to help the team implement the associated guidance. Bookmark this page to come back to this checklist often.

## Before your begin

As you work through this guide, record our foundational decisions using the [initial decision template](#). The template can help you quickly onboard team members who participate in the cloud adoption lifecycle by clarifying how your cloud environment is configured and why.

If you already have an environment running in Azure, the [Azure governance visualizer](#) can help you accelerate your documentation. Gain insight into policies, role-based access control (RBAC), Azure Blueprints, subscriptions, and more. From the collected data the tool provides visibility on your hierarchy map, creates a tenant summary, and builds granular scope insights about management groups and subscriptions.

## Step 1: Understand how Azure works

If you've chosen Azure as a cloud provider to support your cloud adoption journey, it's important to understand [how Azure works](#).

### Involved teams, deliverables, and supporting guidance:

Everyone involved in the cloud adoption lifecycle should have a basic understanding of how Azure works.

## Step 2: Understand initial Azure concepts

Azure is built on a set of [foundational concepts](#) that are required for a deep conversation about the technical strategy for Azure implementations.

### Involved teams, deliverables, and supporting guidance:

Everyone involved in Azure implementation of the technology strategy should understand the terms and definitions in the foundational concepts.

## Step 3: Review the portfolio

Whatever cloud provider you choose, all cloud hosting and environmental decisions start with an understanding of the portfolio of workloads. The Cloud Adoption Framework includes a few tools for understanding and evaluating the portfolio.

### Deliverables:

- Record the location, status, and accountable person for the portfolio documentation in the [initial decision template](#).

#### Guidance to support deliverable completion:

- [Fundamental concepts](#) help you understand key Azure topics before you begin your cloud adoption.
- The [operations management workbook](#) and business alignment approach help you understand the workloads and assets that have been transitioned to a cloud operations team.
- The [cloud adoption plan](#) provides a backlog of the workloads and assets that are slated for adoption in the cloud.
- [Digital estate analysis](#) is an approach to documenting existing workloads and assets that are slated for adoption in the cloud. In Azure, the digital estate is best represented in a tool called [Azure Migrate](#).

ACCOUNTABLE TEAM	RESPONSIBLE AND SUPPORTING TEAMS
<ul style="list-style-type: none"> <li>The cloud strategy team is accountable for defining a way to view the portfolio.</li> </ul>	<ul style="list-style-type: none"> <li>Multiple teams will use the following guidance to create those views. Everyone involved in cloud adoption should know where to find the portfolio view to support decisions later in the process.</li> </ul>

## Step 4: Define portfolio-hierarchy depth to align the portfolio

Hosting assets and workloads in the cloud can be simple, consisting of a single workload and its supporting assets. For other customers, the cloud adoption strategy might include thousands of workloads and many more supporting assets. The portfolio hierarchy gives common names for each level to help create a common language for organization, regardless of the cloud provider.

#### Deliverables:

- Record the relevant hierarchy needs in the [initial decision template](#).

#### Guidance to support deliverable completion:

- Understand the levels of the [portfolio hierarchy](#) to align fundamental terms.

ACCOUNTABLE TEAM	RESPONSIBLE AND SUPPORTING TEAMS
<ul style="list-style-type: none"> <li>The cloud governance team is accountable for defining, enforcing, and automating the portfolio hierarchy to shape corporate policy in the cloud.</li> </ul>	<ul style="list-style-type: none"> <li>Everyone involved in the technical strategy for cloud adoption should be familiar with the portfolio hierarchy and the levels of the hierarchy in use today.</li> </ul>

## Step 5: Establish a naming and tagging standard across the portfolio

All existing workloads and assets should be properly named and tagged in accordance with a naming and tagging standard. Those standards should be documented and available as a reference for all team members. When possible, the standards should also be automatically enforced to ensure minimum tagging requirements.

#### Deliverables:

- Record the location, status, and accountable party for the naming and tagging conventions workbook in the [initial decision template](#).

#### Guidance to support deliverable completion:

- Create a [naming and tagging standard](#).
- Populate the [naming and tagging conventions tracking template](#) to track decisions.
- [Review and update existing tags in Azure](#).
- [Enforce tagging policies in Azure](#).

ACCOUNTABLE TEAM	RESPONSIBLE AND SUPPORTING TEAMS
<ul style="list-style-type: none"> <li>The cloud governance team is accountable for defining, enforcing, and automating the naming and tagging standards to ensure consistency across the portfolio.</li> </ul>	<ul style="list-style-type: none"> <li>Everyone involved in the technical strategy for cloud adoption should be familiar with the naming and tagging standards before deployment to the cloud.</li> </ul>

## Step 6: Create a resource organization design to implement the portfolio hierarchy

To ensure consistent alignment with the portfolio hierarchy decisions, it's important to create a design for resource organization. Such a design aligns organizational tools from the cloud provider with the portfolio hierarchy required to support your cloud adoption plan. This design will guide implementation by clarifying which assets can be deployed into specific boundaries within the cloud environments.

### Deliverables:

- Map Azure products to the aligned level of the portfolio hierarchy in the [initial decision template](#).

### Guidance to support deliverable completion:

- Understand how [Azure products support the portfolio hierarchy](#).
- Review existing subscriptions for alignment to the chosen portfolio hierarchy.

### Build a subscription strategy:

- Start with [two subscriptions by design](#). Add basic subscription designs to account for common enterprise needs, like shared services or sandbox subscriptions.
- [Manage multiple subscriptions](#) as additional subscriptions are required to support the cloud adoption plan.
- Establish [clear boundaries based on the portfolio hierarchy](#).
- When required, [move resource groups and assets between subscriptions](#) to adhere to the organization strategy.

ACCOUNTABLE TEAM	RESPONSIBLE AND SUPPORTING TEAMS
<ul style="list-style-type: none"> <li>The cloud governance team is accountable for defining, implementing, and automating the resource organization design across the portfolio.</li> </ul>	<ul style="list-style-type: none"> <li>Everyone involved in the technical strategy for cloud adoption should be familiar with the resource organization design before deployment to the cloud.</li> </ul>

## Step 7: Map capabilities, teams, and RACI to fundamental concepts

Complexity of the portfolio hierarchy will help inform organizational structures and methodologies to guide the day-to-day activities of various teams.

### Deliverables:

- Complete the getting-started guides for organizational alignment based on these concepts.

### Guidance to support deliverable completion:

- Use the prior steps as a guide to evaluate the [portfolio hierarchy accountability guidance](#). Determine which capabilities might need to be delivered by dedicated organizations or virtual teams.
- Use [Get started: Align your organization](#) to apply the portfolio hierarchy accountability guidance to the RACI (responsible, accountable, consulted, and informed) diagram.

ACCOUNTABLE TEAM	RESPONSIBLE AND SUPPORTING TEAMS
<ul style="list-style-type: none"> <li>The cloud strategy team is accountable for aligning virtual or dedicated organizational structures to ensure success of the cloud adoption lifecycle.</li> </ul>	<ul style="list-style-type: none"> <li>Everyone involved in the cloud adoption lifecycle should be familiar with the alignment of people and levels of accountability.</li> </ul>

## What's next

Build on this set of fundamental concepts through the series of getting-started guides in this section of the Cloud Adoption Framework.

[Apply fundamental concepts to other getting-started guides](#)

# How does Azure work?

11/9/2020 • 2 minutes to read • [Edit Online](#)

Azure is Microsoft's public cloud platform. Azure offers a large collection of services including platform as a service (PaaS), infrastructure as a service (IaaS), and managed database service capabilities. But what exactly is Azure, and how does it work?

Azure, like other cloud platforms, relies on a technology known as *virtualization*. Most computer hardware can be emulated in software, because most computer hardware is simply a set of instructions permanently or semi-permanently encoded in silicon. Using an emulation layer that maps software instructions to hardware instructions, virtualized hardware can execute in software as if it were the actual hardware itself.

Essentially, the cloud is a set of physical servers in one or more datacenters that execute virtualized hardware on behalf of customers. So how does the cloud create, start, stop, and delete millions of instances of virtualized hardware for millions of customers simultaneously?

To understand this, let's look at the architecture of the hardware in the datacenter. Inside each datacenter is a collection of servers sitting in server racks. Each server rack contains many server *blades* as well as a network switch providing network connectivity and a power distribution unit (PDU) providing power. Racks are sometimes grouped together in larger units known as *clusters*.

Within each rack or cluster, most of the servers are designated to run these virtualized hardware instances on behalf of the user. But some of the servers run cloud management software known as a fabric controller. The *fabric controller* is a distributed application with many responsibilities. It allocates services, monitors the health of the server and the services running on it, and heals servers when they fail.

Each instance of the fabric controller is connected to another set of servers running cloud orchestration software, typically known as a *front end*. The front end hosts the web services, RESTful APIs, and internal Azure databases used for all functions the cloud performs.

For example, the front end hosts the services that handle customer requests to allocate Azure resources such as [virtual machines](#), and services like [Azure Cosmos DB](#). First, the front end validates the user and verifies the user is authorized to allocate the requested resources. If so, the front end checks a database to locate a server rack with sufficient capacity and then instructs the fabric controller on that rack to allocate the resource.

So fundamentally, Azure is a huge collection of servers and networking hardware running a complex set of distributed applications to orchestrate the configuration and operation of the virtualized hardware and software on those servers. It is this orchestration that makes Azure so powerful, because users are no longer responsible for maintaining and upgrading hardware because Azure does all this behind the scenes.

## Next steps

Learn more about cloud adoption with the Microsoft Cloud Adoption Framework for Azure.

[Learn about the Microsoft Cloud Adoption Framework for Azure](#)

# Azure fundamental concepts

11/9/2020 • 5 minutes to read • [Edit Online](#)

Learn fundamental concepts and terms that are used in Azure, and how the concepts relate to one another.

## Azure terminology

It's helpful to know the following definitions as you begin your Azure cloud adoption efforts:

- **Resource:** An entity that's managed by Azure. Examples include Azure Virtual Machines, virtual networks, and storage accounts.
- **Subscription:** A logical container for your resources. Each Azure resource is associated with only one subscription. Creating a subscription is the first step in adopting Azure.
- **Azure account:** The email address that you provide when you create an Azure subscription is the Azure account for the subscription. The party that's associated with the email account is responsible for the monthly costs that are incurred by the resources in the subscription. When you create an Azure account, you provide contact information and billing details, like a credit card. You can use the same Azure account (email address) for multiple subscriptions. Each subscription is associated with only one Azure account.
- **Account administrator:** The party associated with the email address that's used to create an Azure subscription. The account administrator is responsible for paying for all costs that are incurred by the subscription's resources.
- **Azure Active Directory (Azure AD):** The Microsoft cloud-based identity and access management service. Azure AD allows your employees to sign in and access resources.
- **Azure AD tenant:** A dedicated and trusted instance of Azure AD. An Azure AD tenant is automatically created when your organization first signs up for a Microsoft cloud service subscription like Microsoft Azure, Intune, or Microsoft 365. An Azure tenant represents a single organization.
- **Azure AD directory:** Each Azure AD tenant has a single, dedicated, and trusted directory. The directory includes the tenant's users, groups, and apps. The directory is used to perform identity and access management functions for tenant resources. A directory can be associated with multiple subscriptions, but each subscription is associated with only one directory.
- **Resource groups:** Logical containers that you use to group related resources in a subscription. Each resource can exist in only one resource group. Resource groups allow for more granular grouping within a subscription, and are commonly used to represent a collection of assets required to support a workload, application, or specific function within a subscription.
- **Management groups:** Logical containers that you use for one or more subscriptions. You can define a hierarchy of management groups, subscriptions, resource groups, and resources to efficiently manage access, policies, and compliance through inheritance.
- **Region:** A set of Azure datacenters that are deployed inside a latency-defined perimeter. The datacenters are connected through a dedicated, regional, low-latency network. Most Azure resources run in a specific Azure region.

## Azure subscription purposes

An Azure subscription serves several purposes. An Azure subscription is:

- **A legal agreement.** Each subscription is associated with an [Azure offer](#), such as a free trial or pay-as-you-go. Each offer has a specific rate plan, benefits, and associated terms and conditions. You choose an Azure offer when you create a subscription.

- **A payment agreement.** When you create a subscription, you provide payment information for that subscription, such as a credit card number. Each month, the costs incurred by the resources deployed to that subscription are calculated and billed via that payment method.
- **A boundary of scale.** Scale limits are defined for a subscription. The subscription's resources can't exceed the set scale limits. For example, there's a limit on the number of virtual machines that you can create in a single subscription.
- **An administrative boundary.** A subscription can act as a boundary for administration, security, and policy. Azure also provides other mechanisms to meet these needs, such as management groups, resource groups, and role-based access control.

## Azure subscription considerations

When you create an Azure subscription, you make several key choices about the subscription:

- **Who is responsible for paying for the subscription?** The party associated with the email address that you provide when you create a subscription by default is the subscription's account administrator. The party associated with this email address is responsible for paying for all costs that are incurred by the subscription's resources.
- **Which Azure offer am I interested in?** Each subscription is associated with a specific [Azure offer](#). You can choose the Azure offer that best meets your needs. For example, if you intend to use a subscription to run nonproduction workloads, you might choose the Pay-As-You-Go Dev/Test offer or the Enterprise Dev/Test offer.

### NOTE

When you sign up for Azure, you might see the phrase *create an Azure account*. You create an Azure account when you create an Azure subscription and associate the subscription with an email account.

## Azure administrative roles

Azure defines three types of roles for administering subscriptions, identities, and resources:

- Classic subscription administrator roles
- Azure role-based access control (RBAC) roles
- Azure Active Directory (Azure AD) administrator roles

The account administrator role for an Azure subscription is assigned to the email account that's used to create the Azure subscription. The account administrator is the billing owner of the subscription. The account administrator can [manage subscription administrators](#) via the Azure portal.

By default, the service administrator role for a subscription also is assigned to the email account that's used to create the Azure subscription. The service administrator has permissions to the subscription equivalent to the RBAC-based Owner role. The service administrator also has full access to the Azure portal. The account administrator can change the service administrator to a different email account.

When you create an Azure subscription, you can associate it with an existing Azure AD tenant. Otherwise, a new Azure AD tenant with an associated directory is created. The role of global administrator in the Azure AD directory is assigned to the email account that's used to create the Azure AD subscription.

An email account can be associated with multiple Azure subscriptions. The account administrator can transfer a subscription to another account.

For a detailed description of the roles defined in Azure, see [Classic subscription administrator roles](#), [Azure RBAC roles](#), and [Azure AD administrator roles](#).

# Subscriptions and regions

Every Azure resource is logically associated with only one subscription. When you create a resource, you choose which Azure subscription to deploy that resource to. You can move a resource to another subscription later.

While a subscription isn't tied to a specific Azure region, each Azure resource is deployed to only one region. You can have resources in multiple regions that are associated with the same subscription.

## NOTE

Most Azure resources are deployed to a specific region. Certain resource types are considered global resources, such as policies that you set by using the Azure Policy services.

## Related resources

The following resources provide detailed information about the concepts discussed in this article:

- [How does Azure work?](#)
- [Resource access management in Azure](#)
- [Azure Resource Manager overview](#)
- [Role-based access control \(RBAC\) for Azure resources](#)
- [What is Azure Active Directory?](#)
- [Associate or add an Azure subscription to your Azure Active Directory tenant](#)
- [Topologies for Azure AD Connect](#)
- [Subscriptions, licenses, accounts, and tenants for Microsoft's cloud offerings](#)

## Next steps

Now that you understand fundamental Azure concepts, learn how to scale with multiple Azure subscriptions.

[Scale with multiple Azure subscriptions](#)

# Understand and align the portfolio hierarchy

11/9/2020 • 11 minutes to read • [Edit Online](#)

Business needs are often supported, improved, or accelerated through information technology. A collection of technologies that delivers defined business value is called a *workload*. That collection might include applications, servers or virtual machines, data, devices, and other similarly grouped assets.

Typically, a business stakeholder and technical leader share accountability for the ongoing support of each workload. In some phases of the workload lifecycle, those roles are clearly stated. In more operational phases of a workload's lifecycle, those roles might be transitioned to a shared operations management team or cloud operations team. As the number of workloads increases, the roles (stated or implied) become more complex and more matrixed.

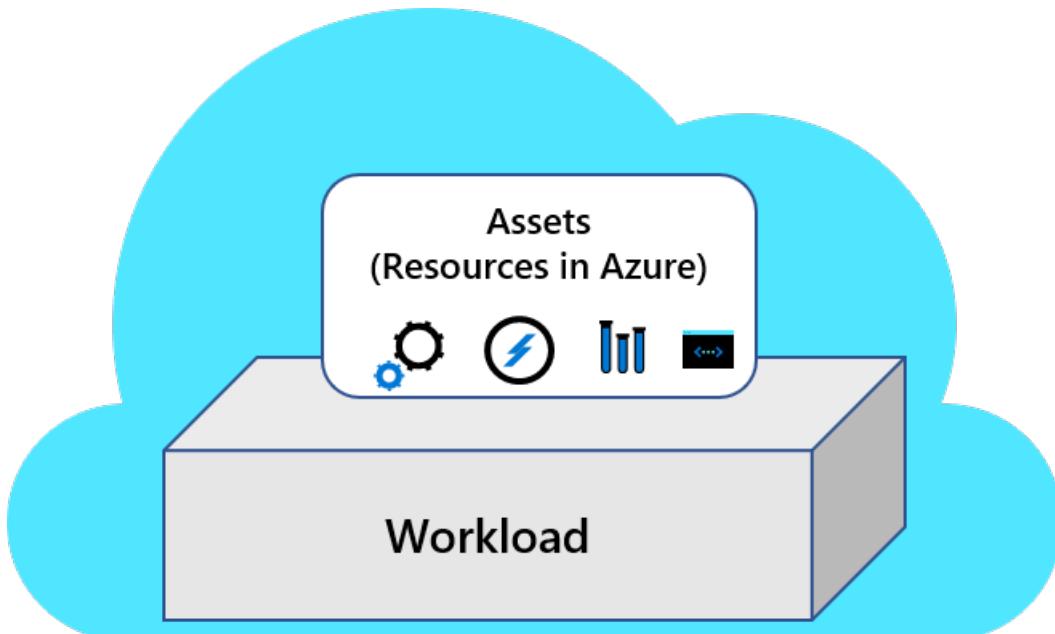
Most businesses rely on multiple workloads to deliver vital business functions. The collection of workloads, assets, and supporting factors (projects, people, processes, and investments) is called a *portfolio*. The matrix of business, development, and operations staff requires a portfolio hierarchy to show how the workloads and supporting services all fit together.

This article provides clear definitions for the levels of the portfolio hierarchy. The article aligns various teams with the appropriate accountability in each layer, along with the source of the best guidance for that team to deliver on the expectations for that level. Throughout this article, each level of the hierarchy is also called a *scope*.

## Portfolio hierarchy

### Workloads

Workloads and their supporting assets are at the core of any portfolio. The additional scopes or layers below define how those workloads are viewed and to what extent they're affected by the matrix of potential supporting teams.



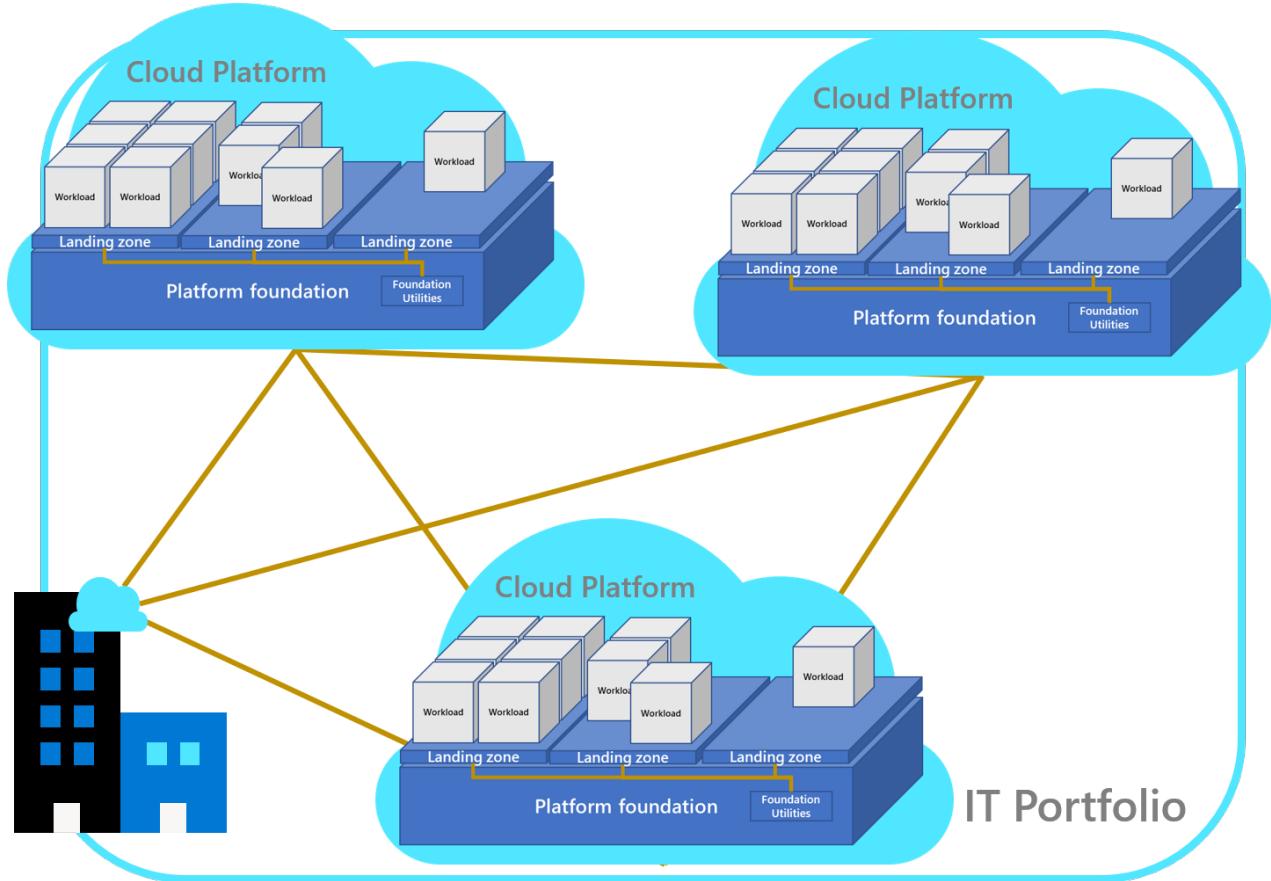
Although the terms can vary, all IT solutions include assets and workloads:

- **Asset:** The smallest unit of technical function that supports a workload or solution.
- **Workload:** The smallest unit of IT support for the business. A workload is a collection of assets (infrastructure, applications, and data) that supports a common business goal or the execution of a common business process.

When you're deploying your first workload, the workload and its assets might be the only defined scope. The other layers might be explicitly defined as more workloads are deployed.

## IT portfolio

When companies support workloads through matrixed approaches or centralized approaches, a broader hierarchy likely exists to support those workloads:



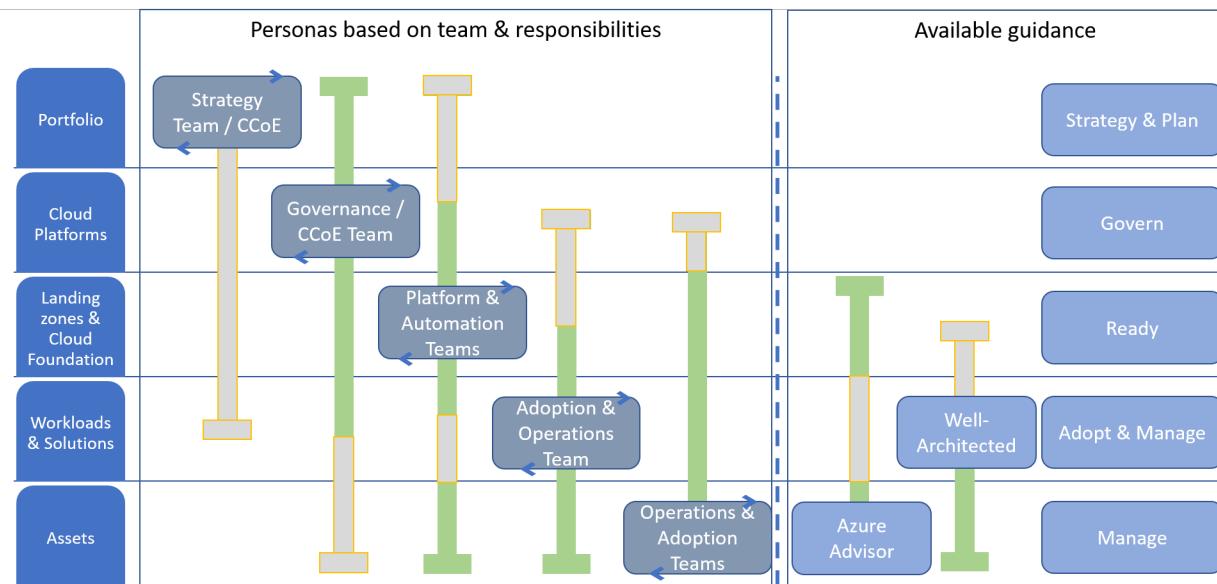
- **Landing zones:** Landing zones provide workloads with the necessary *foundational utilities* (or shared plumbing) that are provided from a *platform foundation* that's required to support one or more workloads. Landing zones are so critical in the cloud that the entire Ready methodology of the Cloud Adoption Framework focuses on landing zones. For a more detailed definition, see [What is a landing zone?](#)
- **Foundational utilities:** These shared IT services are required for workloads to operate within the technology and business portfolio.
- **Platform foundation:** This organizational construct centralizes foundational solutions and helps ensure that those controls are enforced for all landing zones.
- **Cloud platforms:** Depending on the overall strategy for supporting the full *portfolio*, customers might need multiple cloud platforms with distinct deployments of the platform foundation to govern multiple regions, hybrid solutions, or even multicloud solutions.
- **Portfolio:** Through a technology lens, the portfolio is a collection of workloads, assets, and supporting resources that span all cloud platforms. Through a business lens, the portfolio is the collection of projects, people, processes, and investments that support and manage the technology portfolio to drive business outcomes. Together, these two lenses capture the *portfolio*.

## Hierarchy accountability and guidance

An accountable team manages each layer of the portfolio hierarchy. The following diagram shows the mapping between the accountable team and the guidance to support its business decisions, technical decisions, and technical implementation.

## NOTE

The teams mentioned in the following list might be virtual teams or individuals. For some variants of this hierarchy, some of the accountable teams can be collapsed as described later in the accountability variants.



- Portfolio:** The cloud strategy team and the cloud center of excellence (CCoE) use the Strategy and Plan methodologies to guide decisions that affect the overall portfolio. The cloud strategy team is accountable for the enterprise level of the cloud portfolio hierarchy. The cloud strategy team should also be informed of decisions about the environment, landing zones, and high-priority workloads.
- Cloud platforms:** The cloud governance team is accountable for the disciplines that ensure consistency across each environment in alignment with the Govern methodology. The cloud governance team is accountable for governance of all resources in all environments. The cloud governance team should be consulted on changes that might require an exception or change to governing policies. The cloud governance team should also be informed of progress with workload and asset adoption.
- Landing zones and cloud foundation:** The cloud platform team is accountable for developing the landing zones and platform utilities that support adoption. The cloud automation team is accountable for automating the development of, and ongoing support for, those landing zones and platform utilities. Both teams use the Ready methodology to guide implementation. Both teams should be informed of progress with workload adoption and any changes to the enterprise or environment.
- Workloads:** Adoption happens at the workload level. Cloud adoption teams use the Migrate and Innovate methodologies to establish scalable processes to accelerate adoption. After adoption is complete, the ownership of workloads is likely transferred to a cloud operations team that uses the Manage methodology to guide operations management. Both teams should be comfortable using the Microsoft Azure Well-Architected Framework to make detailed architectural decisions that affect the workloads they support. Both teams should be informed of changes to landing zones and environments. Both teams might occasionally contribute to landing zone features.
- Assets:** Assets are typically the responsibility of the cloud operations team. That team uses the management baseline in the Manage methodology to guide operations management decisions. It should also use Azure Advisor and the Azure Well-Architected Framework to make detailed resource and architectural changes that are required to deliver on operations requirements.

## Accountability variants

- Single environment:** When an enterprise needs only one environment, a CCoE is typically not required.
- Single landing zone:** If an environment has only a single landing zone, the governance and platform capabilities can likely be combined into one team.

- **Single workload:** Some businesses need only one workload, or few workloads, in a single landing zone and a single environment. In those cases, there's little need for a separation of duties between governance, platform, and operations teams.

## Common workload and accountability examples

The following examples illustrate the portfolio hierarchy.

### COTS workloads

Traditionally, enterprises have favored commercial-off-the-shelf (COTS) software solutions to power business processes. These solutions are installed, configured, and then operated. There is little change to the solutions architecture after configuration.

In these scenarios, any cloud adoption of COTS solutions ends with a transition to a cloud operations team. The cloud operations team then becomes the technical owner for that software and assumes accountability for managing configuration, cost, patching cycles, and other operational needs.

These workloads include accounting packages, logistics software, or industry-specific solutions. In Microsoft terminology, the vendors of these packages are called independent software vendors (ISVs). Many ISVs offer a service to deploy and maintain an instance of their software package in your subscriptions. They might also offer a version of the software package that runs in their own cloud-hosted environment, providing a platform as a service (PaaS) alternative to the workload.

With the exception of PaaS offerings, cloud operations teams are responsible for ensuring basic operational compliance requirements for those workloads. A cloud operations team should work with the cloud governance team to align cost, performance, and other architecture pillars.

### In development with active revisions

When a COTS solution or PaaS offering isn't aligned to the business need, or no solution exists, enterprises build custom-developed workloads. Typically, a small percentage of the IT portfolio uses this workload approach. But these workloads tend to drive a disproportionately high percentage of IT's contribution to business outcomes, especially outcomes related to new revenue streams. These workloads tend to map well to new innovation ideas.

Given various movements that are rooted in agile methodologies and DevOps practices, these workloads favor a business/DevOps alignment over traditional IT management. For these workloads, there might not be a handoff to the cloud operations team for several years. In those cases, the development team serves as the technical owner of the workload.

Due to extensive time and associated capital constraints, custom development options are often limited to high-value opportunities. Typical examples include application innovations, deep data analysis, or mission-critical business functions.

### Break/fix or sunset development

After a custom-developed workload reaches peak maturity, the development team might be reassigned to other projects. In these cases, technical ownership typically transitions to a cloud operations team. When there's a need for small fixes, the operations team will enlist developers to resolve the error.

In some cases, the development team moves to a project that will eventually replace the current workload. Alternatively, the team might move on because the business opportunity supported by the workload is being phased out. These are examples of sunset scenarios, where the cloud operations team serves as the technical owner until the workload is no longer needed.

In both scenarios, the cloud operations team typically serves as the long-term technical owner and decision maker. That team will likely enlist application developers when operational changes require significant architectural changes.

## Mission-critical workloads

In every company, a few workloads are too important to the business for them to fail. With these mission-critical workloads, there are usually operations and development owners with various levels of responsibility. Those teams should align operational changes and architectural changes to minimize disruptions to the production solution.

These scenarios require a strong focus on separation of duties. To achieve separation of duties, the operations team will generally hold accountability for day-to-day operational changes in the production environment. When those operational changes require an architectural change, they'll be completed by the development or adoption team in a nonproduction environment, before the operations team applies the changes to production.

Examples of mission-critical workloads with a required separation of duties include workloads like SAP, Oracle, or other enterprise resource planning (ERP) solutions, which span multiple business units in the company.

## Strategy portfolio alignment

It's important to understand the strategic objectives of the cloud adoption effort and align the portfolio to support that transformation. A few common types of strategic portfolio alignment help shape the structure of the portfolio hierarchy. The following sections provide examples of the portfolio alignment and impact on the portfolio hierarchy.

### **Innovation or development-led portfolio**

Some companies, especially fast-growing established startups, have a higher-than-average percentage of custom development projects. In development-heavy portfolios, the environment, landing zone, and workloads are often compressed, so there might be specific environments (either production or nonproduction) for specific workloads. This results in a 1:1 ratio between environment, landing zone, and workload.

Because the environment hosts custom solutions, the DevOps pipeline and application-level reporting might replace the need for operations and governance functions. For those customers, a reduced focus on operations, governance, or other supporting roles is likely. A stronger emphasis on the responsibilities of the cloud adoption and cloud automation teams is also typical.

**Portfolio alignment:** The IT portfolio will likely focus on workloads and workload owners to drive critical architecture decisions. Those teams are likely to find more value in the Azure Well-Architected Framework guidance during adoption and operations activities.

**Boundary definitions:** The logical boundaries, even at an enterprise level, will likely focus on production and nonproduction environment segmentation. There might also be clear segmentation between products in the company's software portfolio. At times, there might also be segmentation between development and hosted customer instances.

### **Operations-led portfolio**

Multinational enterprise organizations with more established IT operations teams typically have a stronger focus on governance and operations than development. In these organizations, a higher percentage of workloads typically align to the COTS or break/fix categories, maintained by technical owners within the cloud operations team.

**Portfolio alignment:** The IT portfolio will be workload aligned, but those workloads are then aligned to operating units or business units. There might also be organization around funding models, industry, or other business segmentation requirements.

**Boundary definitions:** Landing zones will likely group applications into application archetypes to keep similar operations in a similar segmentation. Environments will likely refer to physical constructs like datacenter, nation, cloud-provider region, or other operational organization standards.

### **Migration-led portfolio**

Similar to operations-led portfolios, a portfolio that is largely built through migration will be based on specific business drivers that led to the migration of existing assets. Typically, the datacenter is the biggest factor in those drivers.

**Portfolio alignment:** The IT portfolio might be workload aligned, but it's more likely asset aligned. If transitions to IT operations have happened in the company's history, many active-use assets might not be easily mapped to a funded workload. In these cases, many assets might not have a defined workload or clear workload owner until late in the migration process.

**Boundary definitions:** Landing zones will likely group applications into boundaries that reflect on-premises segmentation. Though not a best practice, environments often match the on-premises datacenter name and landing zones that represent network segmentation practices. It's a better practice to adhere to segmentation that more closely aligns with an operations-led portfolio.

### **Governance-led portfolio**

Alignment to governance teams should happen as early as possible. Through governance practices and cloud governance tooling, portfolios and environmental boundaries can best balance the needs of innovation, operations, and migration efforts.

**Portfolio alignment:** Governance-led portfolios tend to include data points that capture innovation and operations details, such as workload, operations owner, data classification, and operational criticality. These data points create a well-rounded view of the portfolio.

**Boundary definitions:** Boundaries in a governance-led portfolio tend to favor operations over innovation, while using a management-group-driven hierarchy that maps to criteria for business units and development environments. At each level of the hierarchy, a cloud governance boundary can have different degrees of policy enforcement to allow for development and creative flexibility. At the same time, production-grade requirements can be applied to production subscriptions to ensure separation of duties and consistent operations.

# How do Azure products support the portfolio hierarchy?

11/9/2020 • 2 minutes to read • [Edit Online](#)

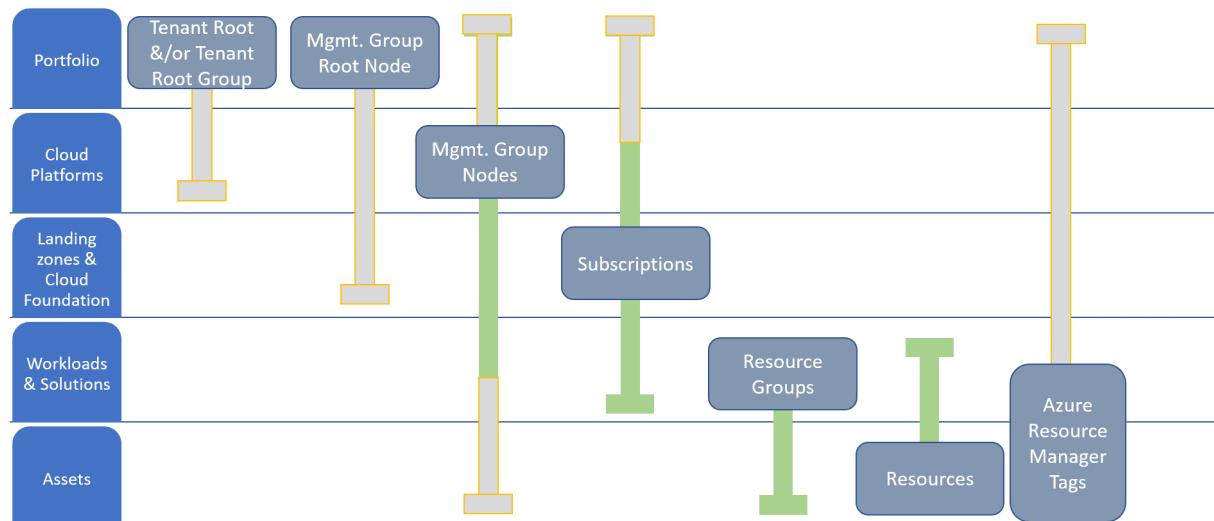
In [Understanding and aligning the portfolio hierarchy](#), a set of definitions for the portfolio hierarchy and role mapping established a hierarchy of scope for most portfolio approaches. As described in that article, you might not need each of the outlined levels or *scopes*. Minimizing the number of layers reduces complexity, so these layers shouldn't all be viewed as a requirement.

This article shows how each level or scope of the hierarchy is supported in Azure through organizational tools, deployment and governance tools, and some solutions in the Microsoft Cloud Adoption Framework for Azure.

## Organizing the hierarchy in Azure

Azure Resource Manager includes several organizational approaches that help organize assets at each level of the cloud hierarchy.

The slide bars in the following diagram demonstrate common variants in alignment. The gray parts of the slide bars are common but should be used only for specific business requirements. The points after the image describe a suggested best practice.



- **Portfolio:** The enterprise or business unit probably won't contain any technical assets but might affect cost decisions. The enterprise and business units are represented in the root nodes of the management group hierarchy.
- **Cloud platforms:** Each environment has its own node in the management group hierarchy.
- **Landing zones and cloud foundation:** Each landing zone is represented as a subscription. Likewise, platform foundations are contained in their own subscriptions. Some subscription designs might call for a subscription per cloud or per workload, which would change the organizing tool for each.
- **Workloads:** Each workload is represented as a resource group. Resource groups are often used to represent solutions, deployments, or other technical groupings of assets.
- **Assets:** Each asset is inherently represented as a resource in Azure.

## Organizing with tags

Deviations from the best practice are common. You can record them by tagging all assets. Use a tag to represent each of the relevant layers of the hierarchy. For more information, see [Recommended naming and tagging conventions](#).

# Get started: Accelerate migration

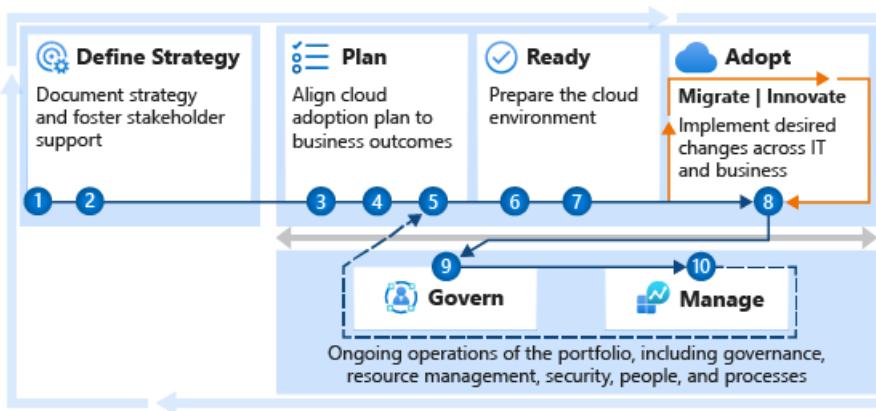
11/9/2020 • 9 minutes to read • [Edit Online](#)

Proper alignment of business and IT stakeholders helps to overcome migration roadblocks and accelerate migration efforts. This article provides recommended steps for:

- Stakeholder alignment
- Migration planning
- Deploying a landing zone
- Migrating your first 10 workloads

It also helps you implement proper governance and management processes.

Use this guide to streamline the processes and materials required for aligning an overall migration effort. The guide uses the methodologies of the Cloud Adoption Framework that are highlighted in this illustration.



If your migration scenario is atypical, you can get a personalized assessment of your organization's migration readiness by using the [strategic migration and readiness tool \(SMART\) assessment](#). Use it to identify the guidance that best aligns to your current needs.

## Get started

The technical effort and process required to migrate workloads is relatively straightforward. It's important to complete the migration process efficiently. Strategic migration readiness has an even bigger impact on the timelines and successful completion of the overall migration.

To accelerate adoption, you must take steps to support the cloud adoption team during migration. This guide outlines these iterative tasks to help customers start on the right path toward any cloud migration. To show the importance of the supporting steps, migration is listed as step 10 in this article. In practice, the cloud adoption team is likely to begin their first pilot migration in parallel with steps 4 or 5.

### Step 1: Align stakeholders

To avoid common migration blockers, create a clear and concise business strategy for migration. Stakeholder alignment on motivations and expected business outcomes shapes decisions made by the cloud adoption team.

- **Motivations:** The first step to strategic alignment is to gain agreement on the motivations that drive the migration effort. Start by understanding and categorizing motivations and common themes from various stakeholders across business and IT.
- **Business outcomes:** After motivations are aligned, it's possible to capture the desired business outcomes. This

information provides clear metrics you can use to measure the overall transformation.

**Deliverables:**

- Use the [strategy and plan template](#) to record motivations and desired business outcomes.

ACCOUNTABLE TEAM	RESPONSIBLE AND SUPPORTING TEAMS
<ul style="list-style-type: none"><li>• Cloud strategy team</li></ul>	<ul style="list-style-type: none"><li>• Cloud adoption team</li><li>• Cloud center of excellence or central IT team</li></ul>

## Step 2: Align partner support

Partners, Microsoft Services, or various Microsoft programs are available to support you throughout the migration process.

- [Understand partnership options](#) to find the right level of partnership and support.

**Deliverables:**

- Establish terms and conditions or other contractual agreements before you engage supporting partners.
- Identify approved partners in the [strategy and plan template](#).

ACCOUNTABLE TEAM	RESPONSIBLE AND SUPPORTING TEAMS
<ul style="list-style-type: none"><li>• Cloud strategy team</li></ul>	<ul style="list-style-type: none"><li>• Cloud adoption team</li><li>• Cloud center of excellence or central IT team</li></ul>

## Step 3: Gather data and analyze assets and workloads

Use discovery and assessment to improve technical alignment and create an action plan for executing your strategy. During this step, validate the business case using data about the current state environment. Then perform quantitative analysis and a deep qualitative assessment of the highest priority workloads.

- **Inventory existing systems:** Use a programmatic data-driven approach to understand the current state. Discover and gather data to enable all assessment activities.
- **Incremental rationalization:** Streamline assessment efforts to focus on a qualitative analysis of all assets, possibly even to support the business case. Then add a deep qualitative analysis for the first 10 workloads to be migrated.

**Deliverables:**

- Raw data on existing inventory.
- Quantitative analysis on existing inventory to refine the business justification.
- Qualitative analysis of the first 10 workloads.
- Business justification documented in the [strategy and plan template](#).

ACCOUNTABLE TEAM	RESPONSIBLE AND SUPPORTING TEAMS
<ul style="list-style-type: none"><li>• Cloud adoption team</li></ul>	<ul style="list-style-type: none"><li>• Cloud strategy team</li></ul>

## Step 4: Make a business case

Making the business case for migration is likely to be an iterative conversation among stakeholders. In this first pass at building the business case, evaluate the initial high-level return from a potential cloud migration. The goal of this step is to ensure that all stakeholders align around one simple question: based on the available data, is the overall adoption of the cloud a wise business decision?

- [Building a cloud migration business case](#) is a good starting point for developing a migration business case. Clarity on formulas and tools can aid in business justification.

### Deliverables:

- Use the [strategy and plan template](#) to record business justification.

ACCOUNTABLE TEAM	RESPONSIBLE AND SUPPORTING TEAMS
• Cloud strategy team	• Cloud adoption team

## Step 5: Create a migration plan

A cloud adoption plan provides an accelerated approach to developing a project backlog. The backlog can then be modified to reflect discovery results, rationalization, needed skills, and partner contracting.

- [Cloud adoption plan](#): Define your cloud adoption plan using the basic template.
- [Workload alignment](#): Define workloads in the backlog.
- [Effort alignment](#): Align assets and workloads in the backlog to clearly define effort for prioritized workloads.
- [People and time alignment](#): Establish iteration, velocity (people's time), and releases for the migrated workloads.

### Deliverables:

- Deploy the backlog template.
- Update the template to reflect the first 10 workloads to be migrated.
- Update people and velocity to estimate release timing.
- Timeline risks:
  - Lack of familiarity with Azure DevOps can slow the deployment process.
  - Complexity and data available for each workload can also affect timelines.

ACCOUNTABLE TEAM	RESPONSIBLE AND SUPPORTING TEAMS
• Cloud adoption team	• Cloud strategy team

## Step 6: Build a skills readiness plan

Existing employees can play a hands-on role in the migration effort, but additional skills might be required. In this step, find ways to develop those skills or use partners to add to those skills.

- [Build a skills-readiness plan](#). Quickly evaluate your existing skills to identify what other skills the team should develop.

### Deliverables:

- Add a skills-readiness plan to the [strategy and plan template](#).

ACCOUNTABLE TEAM	RESPONSIBLE AND SUPPORTING TEAMS
• Cloud adoption team	• Cloud strategy team

## Step 7: Deploy and align a landing zone

All migrated assets are deployed to a landing zone. The landing zone starts simple to support smaller workloads, then scales to address more complex workloads over time.

- [Choose a landing zone](#): Find the right approach to deploying a landing zone based on your adoption pattern. Then deploy that standardized code base.
- [Expand your landing zone](#): Whatever your starting point, identify gaps in the deployed landing zone and add required components for resource organization, security, governance, compliance, and operations.

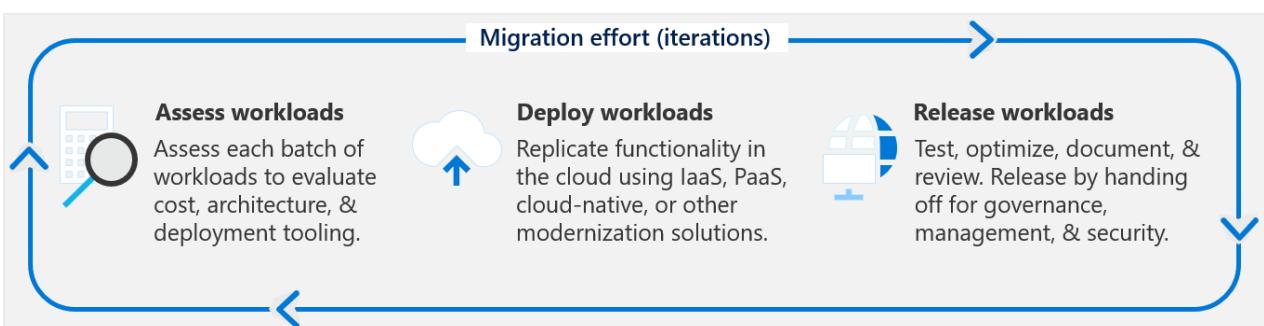
### Deliverables:

- Deploy your first landing zone for deploying initial low-risk migrations.
- Develop a refactoring plan with the cloud center of excellence or the central IT team.
- Timeline risks:
  - Governance, operations, and security requirements for the first 10 workloads can slow this process.
  - Refactoring the first landing zone and subsequent landing zones takes longer, but it should happen in parallel with migration efforts.

ACCOUNTABLE TEAM	RESPONSIBLE AND SUPPORTING TEAMS
• Cloud platform team	• Cloud adoption team • Cloud center of excellence or central IT team

## Step 8: Migrate your first 10 workloads

The technical effort required to migrate your first 10 workloads is relatively straightforward. It's also an iterative process that you repeat as you migrate more assets. In this process, you assess your workloads, deploy your workloads, and then release them to your production environment.



Cloud migration tools enable migrating all virtual machines in a datacenter in one pass or iteration. It's more common to migrate a smaller number of workloads during each iteration. Breaking up the migration into smaller increments requires more planning, but it reduces technical risks and the impact of organizational change management.

With each iteration, the cloud adoption team gets better at migrating workloads. These steps help the technical

team mature their capabilities:

1. Migrate your first workload in a pure infrastructure as a service (IaaS) approach by using the tools outlined in the [Azure migration guide](#).
2. Expand tooling options to use migration and modernization by using the [migration examples](#).
3. Develop your technical strategy by using broader approaches outlined in [Azure cloud migration best practices](#).
4. Improve consistency, reliability, and performance through an efficient migration-factory approach as outlined in [Migration process improvements](#).

#### Deliverables:

Continuous improvement of the adoption team's ability to migrate workloads.

ACCOUNTABLE TEAM	RESPONSIBLE AND SUPPORTING TEAMS
<ul style="list-style-type: none"><li>Cloud adoption team</li></ul>	<ul style="list-style-type: none"><li>Cloud strategy team</li><li>Cloud center of excellence or central IT team</li></ul>

## Step 9: Hand off production workloads to cloud governance

Governance is a key factor to the long-term success of any migration effort. Speed to migration and business impact is important. But speed without governance can be dangerous. Your organization needs to make decisions about governance that align to your adoption patterns and your governance and compliance needs.

- [Governance approach](#): This methodology outlines a process for thinking about your corporate policy and processes. After determining your approach, you can build the disciplines required to enable governance across your enterprise cloud adoption efforts.
- [Initial governance foundation](#): Understand the disciplines needed to create a governance minimum viable product (MVP) that serves as the foundation for all adoption.
- [Governance benchmark](#): Identify gaps in your organization's current state of governance. Get a personalized benchmark report and curated guidance on how to get started.

#### Deliverables:

- Deploy an initial governance foundation.
- Complete a governance benchmark to plan for future improvements.
- Timeline risk:
  - Improvement of policies and governance implementation can add one to four weeks per discipline.

ACCOUNTABLE TEAM	RESPONSIBLE AND SUPPORTING TEAMS
<ul style="list-style-type: none"><li>Cloud governance team</li></ul>	<ul style="list-style-type: none"><li>Cloud strategy team</li><li>Cloud center of excellence or central IT team</li></ul>

## Step 10: Hand off production workloads to cloud operations

Operations management is another requirement to reach migration success. Migrating individual workloads to the cloud without an understanding of ongoing enterprise operations is a risky decision. In parallel with migration, you should start planning for longer-term operations.

- [Establish a management baseline](#)

- Define business commitments
- Expand the management baseline
- Get specific with advanced operations

#### Deliverables:

- Deploy a management baseline.
- Complete the operations management workbook.
- Identify any workloads that require an Microsoft Azure Well-Architected Review assessment.
- Timeline risks:
  - Review the workbook: estimate one hour per application owner.
  - Complete the Microsoft Azure Well-Architected Review assessment: estimate one hour per application.

ACCOUNTABLE TEAM	RESPONSIBLE AND SUPPORTING TEAMS
<ul style="list-style-type: none"> <li>● Cloud operations team</li> </ul>	<ul style="list-style-type: none"> <li>● Cloud strategy team</li> <li>● Cloud center of excellence or central IT team</li> </ul>

## Value statement

These steps help teams accelerate their migration efforts through better change management and stakeholder alignment. These steps also remove common blockers and realize business value more quickly.

## Next steps

The Cloud Adoption Framework is a lifecycle solution that helps you begin a migration journey. It also helps mature the teams that support migration efforts. The following teams can use these next steps to continue to mature their capabilities. These parallel processes aren't linear and shouldn't be considered blockers. Instead, each is a parallel value stream to help improve your organization's overall cloud readiness.

TEAM	NEXT ITERATION
Cloud adoption team	Use the <a href="#">migration model</a> to learn about moving toward a migration factory that provides efficient ongoing migration capabilities.
Cloud strategy team	Iteratively improve the <a href="#">Strategy methodology</a> and the <a href="#">Plan methodology</a> along with the adoption plan. Review these overviews and continue iterating on your business and technical strategies.
Cloud platform team	Revisit the <a href="#">Ready methodology</a> to continue to advance the overall cloud platform that supports migration or other adoption efforts.
Cloud governance team	Use the <a href="#">Govern methodology</a> to continue to improve governance processes, policies, and disciplines.
Cloud operations team	Build on the <a href="#">Manage methodology</a> to provide richer operations in Azure.

If your migration scenario is atypical, you can get a personalized assessment of your organization's migration readiness by using the [strategic migration and readiness tool \(SMART\) assessment](#). The answers you provide help

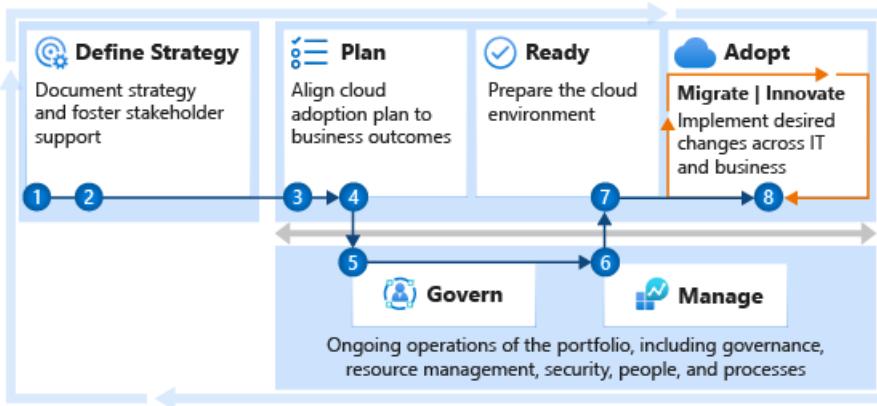
identify which guidance aligns best with your current needs.

# Get started: Accelerate new product and service innovation in the cloud

11/9/2020 • 10 minutes to read • [Edit Online](#)

Creating new products and services in the cloud requires a different approach than migration requires. The Innovate methodology of the Cloud Adoption Framework establishes an approach that guides the development of new products and services.

This guide uses the sections of the Cloud Adoption Framework that are highlighted in the following illustration. Innovation is less predictable than a standard migration, but it still fits within the context of the broader cloud adoption plan. This guide can help your enterprise provide the support needed to innovate and provide a structure for creating a balanced portfolio throughout cloud adoption.



## Step 1: Document the business strategy

To avoid common blockers, create a clear and concise business strategy for innovation. Stakeholder alignment on motivations and expected business outcomes shapes decisions that the cloud adoption team makes.

### Deliverables:

- Use the [strategy and plan template](#) to record motivations and desired business outcomes.

### Guidance to support deliverable completion:

- **Motivations:** The first step to strategic alignment is to gain agreement on the motivations that drive the innovation effort. Start by understanding and categorizing motivations and common themes from stakeholders across business and IT.
- **Business outcomes:** After motivations are aligned, it's possible to capture the desired business outcomes. This information provides clear metrics that you can use to measure the overall transformation.
- **Balancing the portfolio:** Innovation isn't the right adoption path for every workload. This approach to adoption is more relevant to new custom-built applications or workloads that *require* rearchitecture or full rebuilds. When motivations heavily favor innovation for all workloads, it's important to evaluate the portfolio to ensure that those investments can produce the desired return on investment. Modernization of specific resources and small-scale rebuilding efforts can be innovative but might be better served by following [Get started: Accelerate migration](#).

ACCOUNTABLE TEAM	RESPONSIBLE AND SUPPORTING TEAMS
<ul style="list-style-type: none"> <li>Cloud strategy team</li> </ul>	<ul style="list-style-type: none"> <li>Cloud adoption team</li> <li>Cloud center of excellence or central IT team</li> </ul>

## Step 2: Evaluate the business justification

In this first pass at building the business case, evaluate the initial high-level return from a potential cloud adoption effort. The goal of this step is to align all stakeholders around one simple question: based on the available data, is the overall adoption of the cloud a wise business decision? Building on that question, the team can better align on how this innovation project helps meet the users' projected needs within the goal of adopting the cloud.

### Deliverables:

- Use the [strategy and plan template](#) to record the business justification.

### Guidance to support deliverable completion:

- Business justification:** Before you evaluate each opportunity to innovate in the cloud, complete a high-level business justification to establish stakeholder alignment for the overall adoption plan.
- Business value consensus:** Quantifying the value of an innovation can be difficult early in the process. The exercise in this article can aid in evaluating alignment on the business value of a specific innovation effort.

ACCOUNTABLE TEAM	RESPONSIBLE AND SUPPORTING TEAMS
<ul style="list-style-type: none"> <li>Cloud strategy team</li> </ul>	<ul style="list-style-type: none"> <li>Cloud adoption team</li> </ul>

## Step 3: Gather data and analyze assets and workloads

In most enterprises, innovation can be accelerated through the use of existing assets like applications, virtual machines (VMs), and data. When you plan for innovation, it's important to understand how and when those assets are migrated to the cloud.

### Deliverables:

- Get raw data on existing inventory like applications, VMs, and data.
- If the proposed innovation has dependencies on existing inventory, complete the following deliverables:
  - Quantitative analysis on any supporting inventory required to support the planned innovation.
  - Qualitative analysis of any supporting workloads required to deliver the innovation.
- Calculate the cost of new inventory required to support the innovation effort.
- Update the business justification in the [strategy and plan template](#) with refined calculations.

### Guidance to support deliverable completion:

Discovery and assessment provide a deeper level of technical alignment. You can then create an action plan for migrating any dependent workloads that the planned innovation requires. This scenario is common when companies have existing data sources, centralized applications, or service layers that are necessary for delivering innovation within the context of the rest of the enterprise.

When there are dependent systems, the following articles can guide the discovery and assessment:

- Inventory existing systems:** Understanding the current state from a programmatic, data-driven approach is the first step. Discover and gather data to enable all assessment activities.

- **Incremental rationalization:** Streamline assessment efforts to focus on a qualitative analysis of all assets, possibly even to support the business case. Then add a deep qualitative analysis for the first 10 workloads.

ACCOUNTABLE TEAM	RESPONSIBLE AND SUPPORTING TEAMS
• Cloud adoption team	• Cloud strategy team

## Step 4: Plan for migration of dependent assets

When new innovation depends on existing workloads or assets, a cloud adoption plan provides an accelerated approach to developing a project backlog. The backlog can then be modified to reflect discovery results, rationalization, needed skills, and partner contracting.

### Deliverables:

- Deploy the backlog template.
- Update the template to reflect the first 10 workloads to be migrated.
- Update people and velocity (people's time) to estimate release timing.
- Timeline risks:
  - Lack of familiarity with Azure DevOps can slow the deployment process.
  - Complexity and data available for each workload can also affect timelines.

### Guidance to support deliverable completion:

- **Cloud adoption plan:** Define your plan using the basic template.
- **Workload alignment:** Define workloads in the backlog.
- **Effort alignment:** Align assets and workloads in the backlog to clearly define the effort for prioritized workloads.
- **People and time alignment:** Establish iteration, velocity, and releases for the workloads.

ACCOUNTABLE TEAM	RESPONSIBLE AND SUPPORTING TEAMS
• Cloud adoption team	• Cloud strategy team

## Step 5: Align governance requirements to your adoption plan

Discussing planned innovations with the governance team helps you avoid many blockers before they arise. Sometimes, innovative new solutions might require practices that are discouraged in sound governance practices. Some of those required features might even be blocked through automated tooling for governance enforcement.

### Deliverables:

- Create transparency and understanding between innovation needs and governance constraints.
- When necessary, update policies and processes to reflect any changes or exceptions to existing governance constraints.

### Guidance to support deliverable completion:

These links help the adoption team understand the approach of the cloud governance team:

- **Governance approach:** This methodology outlines a process for thinking about corporate policy and processes.

Then you can build the disciplines required to deliver on governance across your cloud enterprise efforts.

- [Definition of corporate policy](#): Identify and mitigate business risks.

ACCOUNTABLE TEAM	RESPONSIBLE AND SUPPORTING TEAMS
<ul style="list-style-type: none"><li>• Cloud governance team</li><li>• Cloud adoption team</li></ul>	<ul style="list-style-type: none"><li>• Cloud strategy team</li><li>• Cloud center of excellence or central IT team</li></ul>

## Step 6: Define operational needs and business commitments

Define the plan for long-term operational responsibilities for the planned innovation. Will the established management baseline meet your operational needs? If not, evaluate options for funding operations that are specific to the technology that supports this innovation.

### Deliverables:

- Complete the [Microsoft Azure Architecture Review](#) to assess various architecture and operation decisions.
- Adjust the [operations management workbook](#) to reflect any required advanced operations.

### Guidance to support deliverable completion:

- [Expand the management baseline](#): This section of the Cloud Adoption Framework guides you through various transitions into operational management in the cloud.
- [Get specific with advanced operations](#): Discover ways to go beyond your management baseline.
- If advanced operations are required to support your operations needs, evaluate the [business commitments](#) to determine operational responsibilities for both teams.

ACCOUNTABLE TEAM	RESPONSIBLE AND SUPPORTING TEAMS
<ul style="list-style-type: none"><li>• Cloud operations team</li><li>• Cloud adoption team</li></ul>	<ul style="list-style-type: none"><li>• Cloud strategy team</li><li>• Cloud center of excellence or central IT team</li></ul>

## Step 7: Deploy an aligned landing zone

All assets hosted in the cloud live within a landing zone. That landing zone might have explicit governance, security, and operational requirements. Or, it might be a new subscription without support from other teams. In either scenario, it's important to start with a landing zone that aligns to governance and operational requirements from the beginning.

Starting with an approved landing zone helps your team to discover policy violations early during development versus when the solution is released to production. Early discovery helps your team to remove blockers and gives adoption and governance teams enough time to make changes.

### Deliverables:

- Deploy a first landing zone for initial, low-risk experimentation during early innovation.
- Develop a plan to refactor with the cloud center of excellence or the central IT team to ensure governance, security, and operational alignment.
- Timeline risks:
  - Governance, operations, and security requirements for the first 10 workloads can slow this process. Refactoring the first landing zone and later landing zones takes longer, but it should happen in parallel

with migration efforts.

#### Guidance to support deliverable completion:

- [Choose a landing zone](#): Use this section to find the right approach to deploying a landing zone based on your adoption pattern. Then deploy that standardized code base.
- [Expand your landing zone](#): Regardless of the starting point, identify gaps in the deployed landing zone to add required components for resource organization, security, governance, compliance, and operations.

ACCOUNTABLE TEAM	RESPONSIBLE AND SUPPORTING TEAMS
<ul style="list-style-type: none"><li>• Cloud platform team</li><li>• Cloud adoption team</li></ul>	<ul style="list-style-type: none"><li>• Cloud adoption team</li><li>• Cloud center of excellence or central IT team</li></ul>

## Step 8: Innovate in the cloud

The Innovate methodology provides guidance on the tools and product management approaches most commonly used to innovate in the cloud. These steps help you get started with this approach.

#### Deliverables:

- Technology-based solutions that enrich your customers' lives and drive value for the business.
- Processes and tools to iterate on those solutions faster and add more value by using the cloud:
  - Iterative development approaches.
  - Custom-built applications.
  - Technology-based experiences.
  - Integration of physical products and technology by using IoT.
  - Ambient intelligence: integration of nonintrusive technology into an environment.
  - Azure Cognitive Services: big data, AI, machine learning, and predictive solutions.

#### Guidance to support deliverable completion:

- [Business value consensus](#): If more than three months have passed since the last business value consensus, or if one was never completed, start here.
- [Azure innovation guide](#): Use the Azure innovation guide to speed up the deployment of innovative solutions by understanding the tools and processes that can help you create a minimum viable product (MVP).
- [Innovation best practices](#): Combine Azure services to create a toolchain for digital invention.
- [Feedback loops](#): Develop improved feedback loops to quickly deliver impactful innovations to your customers.

## Step 9: Assess the innovation maturity of your organization

To support the development of your innovation strategy, the AI Maturity Model is a free tool that helps organizations assess their ability to create and own AI-based systems. There are four levels of maturity: foundational, approaching, aspirational, and mature. Each level includes a specific set of characteristics to help determine your organization's ability to adopt specific types of AI solutions, mitigate associated risks, and implement strategies.

The assessment takes 5 to 10 minutes and measures your organization's capability across four categories: strategy, culture, organizational characteristics, and capabilities. Measuring these categories allows the AI Maturity Model to compute your organization's score and provide an estimate of the AI innovation maturity on a curve.

#### Deliverables:

- Use the [AI Maturity Model tool](#) to assess your organization's AI maturity to create AI-based systems.

#### Guidance to support deliverable completion:

- When the assessment is complete, the tool's output will provide a score that estimates the status of AI innovation maturity.

ACCOUNTABLE TEAM	RESPONSIBLE AND SUPPORTING TEAMS
<ul style="list-style-type: none"> <li>• Cloud adoption team</li> </ul>	<ul style="list-style-type: none"> <li>• Cloud center of excellence</li> <li>• Cloud center of excellence or central IT team</li> </ul>

## Value statement

The steps outlined in this guide can help you and your teams create innovative solutions in the cloud that create business value, are governed appropriately, and are well architected.

## Next steps

The Cloud Adoption Framework is a lifecycle solution. It can help you begin an innovation journey. It can help your organization to start an innovation journey and to advance the maturity of the teams that support innovation efforts.

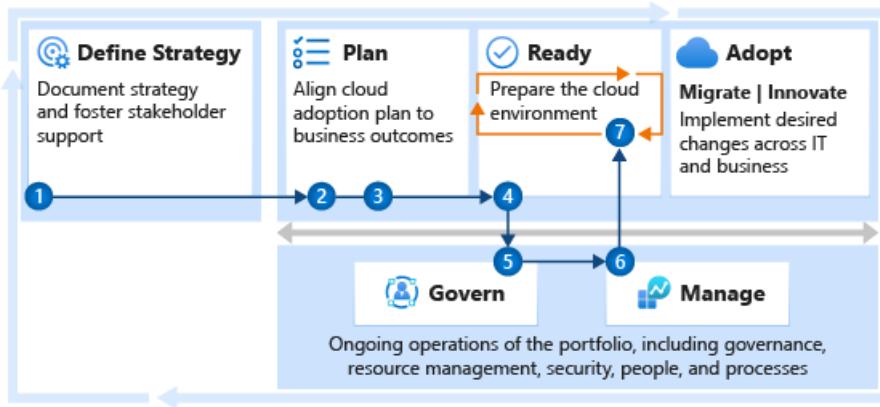
The following teams can use these next steps to continue to advance the maturity of their efforts. These parallel processes aren't linear and shouldn't be viewed as blockers. Instead, each is a parallel value stream to help mature your company's overall cloud readiness.

TEAM	NEXT ITERATION
Cloud adoption team	<a href="#">Process improvements</a> provide insight about approaches to deliver on innovations that affect customers and drive recurring adoption.
Cloud strategy team	The <a href="#">Strategy methodology</a> and the <a href="#">Plan methodology</a> are iterative processes that evolve with the adoption plan. Return to these overview pages and continue to iterate on your business and technical strategies.
Cloud platform team	Revisit the <a href="#">Ready methodology</a> to continue to advance the overall cloud platform that supports migration or other adoption efforts.
Cloud governance team	Use the <a href="#">Govern methodology</a> to continue to improve governance processes, policies, and disciplines.
Cloud operations team	Build on the <a href="#">Manage methodology</a> to provide richer operations in Azure.

# Get started: Environment design and configuration

11/9/2020 • 7 minutes to read • [Edit Online](#)

Environment design and configuration are the most common blockers to adoption efforts that are focused on migration or innovation. Quickly implementing a design that supports your long-term adoption plan can be difficult. This article establishes an approach and series of steps that help to overcome common blockers and accelerate your adoption efforts.



The technical effort required to create an effective environmental design and configuration can be complex. You can manage the scope to improve the odds of success for the cloud platform team. The greatest challenge is alignment among multiple stakeholders. Some of these stakeholders have the authority to stop or slow the adoption efforts. These steps outline ways to quickly meet short-term objectives and establish long-term success.

## Step 1: Document the business strategy

To avoid common migration blockers, make sure that you have a clear and concise business strategy. Stakeholder alignment on motivations, expected business outcomes, and the business justification is important throughout adoption and environment configuration.

A clear and concise business strategy helps the cloud platform team understand what's important and what should be prioritized when they're making environmental configuration decisions. In particular, it helps the teams make decisions when they're forced to choose between speed of innovation or adherence to controls.

### Deliverables:

- Use the [strategy and plan template](#) to record motivations, desired business outcomes, and high-level business justification.

### Guidance to support deliverable completion:

- **Understand business motivations:** The first step to strategic alignment is to agree on the motivations that drive the migration effort. Start by understanding and categorizing motivations and common themes from various stakeholders across business and IT.
- **Document business outcomes:** After motivations are aligned, you can capture the desired business outcomes. This information provides clear metrics you can use to measure the overall transformation.
- **Build a cloud migration business case:** Start developing a business case for migration, including clear guidance on the formulas and tools that help your business justification.

ACCOUNTABLE TEAM	RESPONSIBLE AND SUPPORTING TEAMS	INFORMED TEAMS
<ul style="list-style-type: none"> <li>Cloud strategy team</li> </ul>	<ul style="list-style-type: none"> <li>Cloud adoption team</li> <li>Cloud center of excellence or central IT team</li> </ul>	<ul style="list-style-type: none"> <li>Cloud platform team</li> </ul>

## Step 2: Assess the digital estate

Discovery and assessment provide a deeper level of technical alignment, which helps you create an action plan you can use to deliver on the strategy. During this step, you validate the business case by using data about the current state of the environment. Then you perform quantitative analysis of that data and a deep qualitative assessment of the highest priority workloads.

The output of the digital estate assessment provides the cloud platform team with a clear view of the end-state environment and the requirements that are needed to support the adoption plan.

### Deliverables:

- Raw data on the existing inventory.
- Quantitative analysis of the existing inventory to refine the business justification.
- Qualitative analysis of the first 10 workloads.
- Updated business justification in the [strategy and plan template](#).

### Guidance to support deliverable completion:

- Inventory existing systems:** Understanding the current state from a programmatic, data-driven approach is the first step. Find and gather data to enable all assessment activities.
- Incremental rationalization:** Streamline assessment efforts to focus on a qualitative analysis of all assets, possibly even to support the business case. Then add a deep qualitative analysis for the first 10 workloads to be migrated.

ACCOUNTABLE TEAM	RESPONSIBLE AND SUPPORTING TEAMS	INFORMED TEAMS
<ul style="list-style-type: none"> <li>Cloud adoption team</li> </ul>	<ul style="list-style-type: none"> <li>Cloud strategy team</li> </ul>	<ul style="list-style-type: none"> <li>Cloud platform team</li> </ul>

## Step 3: Create a cloud adoption plan

Your cloud adoption plan provides an accelerated approach to developing a project backlog. The backlog can then be modified to reflect assessment results, rationalization, needed skills, and partner contracting.

A review of the short-term cloud adoption plan and backlog helps the cloud platform team understand the needs of the environment for the next few months. This background helps them to tighten the "definition of done" for the first few landing zones.

### Deliverables:

- Deploy the backlog template.
- Update the template to reflect the first 10 workloads to be migrated.
- Update people and velocity (people's time) to estimate release timing.
- Timeline risks:
  - Lack of familiarity with Azure DevOps can slow the deployment process.

- Complexity and data available for each workload can also affect timelines.

#### Guidance to support deliverable completion:

- Cloud adoption plan:** Define your plan using the basic template.
- Workload alignment:** Define workloads in the backlog.
- Effort alignment:** Align assets and workloads in the backlog to clearly define efforts for prioritized workloads.
- People and time alignment:** Establish iteration, velocity, and releases for the migrated workloads.

ACCOUNTABLE TEAM	RESPONSIBLE AND SUPPORTING TEAMS	INFORMED TEAMS
<ul style="list-style-type: none"> <li>Cloud adoption team</li> </ul>	<ul style="list-style-type: none"> <li>Cloud strategy team</li> <li>Cloud platform team</li> </ul>	<ul style="list-style-type: none"> <li>Cloud platform team</li> </ul>

## Step 4: Deploy the first landing zone

Initially, the cloud adoption team needs a landing zone that can support the requirements of the first wave of workloads. Over time, the landing zone scales to address more complex workloads. For now, start with a landing zone that enables early learning for the cloud platform team and the cloud adoption team.

#### Deliverables:

- Deploy a first landing zone for initial low-risk migrations.
- Develop a plan to refactor with the cloud center of excellence or the central IT team.
- Timeline risks:
  - Governance, operations, and security requirements for the first 10 workloads can slow this process. Actual refactoring of the first landing zone and subsequent landing zones takes longer, but it should happen in parallel with migration efforts.

#### Guidance to support deliverable completion:

- Choose a landing zone:** Use this section to find the right approach to deploying a landing zone based on your short-term adoption plan. Then deploy that standardized code base.
- Expand your landing zone:** Don't attempt to meet long-term governance, security, or operation constraints yet, unless they're required to support the short-term adoption plan.

ACCOUNTABLE TEAM	RESPONSIBLE AND SUPPORTING TEAMS
<ul style="list-style-type: none"> <li>Cloud platform team</li> </ul>	<ul style="list-style-type: none"> <li>Cloud adoption team</li> <li>Cloud center of excellence or central IT team</li> </ul>

## Step 5: Deploy an initial governance foundation

Governance is a key factor to the long-term success of any migration effort. Speed to migration and business impact is important. But speed without governance can be dangerous. Your organization needs to make decisions about governance that align to your adoption patterns and your governance and compliance needs.

As those decisions are made, they feed back into the parallel efforts of the cloud platform team.

#### Deliverables:

- Deploy an initial governance foundation.
- Complete a governance benchmark to plan for future improvements.
- Timeline risks:
  - Improvement of policies and governance implementation can add one to four weeks per discipline.

#### Guidance to support deliverable completion:

- [Governance approach](#): This methodology outlines a process for thinking about corporate policy and processes. Then build the disciplines required to deliver on governance across your cloud enterprise adoption efforts.
- [Governance benchmark tool](#): Find gaps in your current state so that you can plan for the future.
- [Initial governance foundation](#): Understand the governance disciplines that are required to create a governance minimum viable product (MVP) to serve as the foundation for all adoption.

ACCOUNTABLE TEAM	RESPONSIBLE AND SUPPORTING TEAMS	CONSULTED TEAMS
<ul style="list-style-type: none"> <li>• Cloud governance team</li> </ul>	<ul style="list-style-type: none"> <li>• Cloud strategy team</li> <li>• Cloud center of excellence or central IT team</li> </ul>	<ul style="list-style-type: none"> <li>• Cloud platform team</li> </ul>

## Step 6: Implement an operations baseline

Migrating to the cloud without understanding ongoing operations is risky. In parallel with migration, start planning for longer-term operations management. Feed those plans back into the parallel efforts of the cloud platform team.

#### Deliverables:

- Deploy a management baseline.
- Complete the operations management workbook.
- Identify any workloads that require an Microsoft Azure Well-Architected Review assessment.
- Timeline risks:
  - Review the workbook: estimate one hour per application owner.
  - Complete the Microsoft Azure Well-Architected Review assessment: estimate one hour per application.

#### Guidance to support deliverable completion:

- [Establish a management baseline](#)
- [Define business commitments](#)
- [Expand the management baseline](#)
- [Get specific with advanced operations](#)

ACCOUNTABLE TEAM	RESPONSIBLE AND SUPPORTING TEAMS	CONSULTED TEAMS
<ul style="list-style-type: none"> <li>• Cloud operations team</li> </ul>	<ul style="list-style-type: none"> <li>• Cloud strategy team</li> <li>• Cloud center of excellence or central IT team</li> </ul>	<ul style="list-style-type: none"> <li>• Cloud platform team</li> </ul>

## Step 7: Expand the landing zone

As the cloud adoption team begins their first few migrations, the cloud platform team can begin building toward

the end-state environment configuration with the support of the cloud governance and cloud operations teams. Depending on the pace of the cloud adoption plan, this process might need to happen in iterative releases. Functionality might be added ahead of the requirements of the adoption plan.

#### Deliverables:

- Adopt a test-driven development approach to refactoring landing zones.
- Improve landing zone governance.
- Expand landing zone operations.
- Implement landing zone security.

#### Guidance to support deliverable completion:

- [Refactor landing zones](#)
- [Test-driven development of landing zones](#)
- [Expand landing zone governance](#)
- [Expand landing zone operations](#)
- [Expand landing zone security](#)

ACCOUNTABLE TEAM	RESPONSIBLE AND SUPPORTING TEAMS
<ul style="list-style-type: none"><li>• Cloud platform team</li></ul>	<ul style="list-style-type: none"><li>• Cloud adoption team</li><li>• Cloud center of excellence or central IT team</li></ul>

## Value statement

The steps outlined in this guide can help you and your teams accelerate their path to an enterprise-ready cloud environment that's properly configured.

## Next steps

Consider these next steps in a future iteration to build on your initial efforts:

- [Environmental technical readiness learning paths](#)
- [Migration environment planning checklist](#)

# Enable customer success with a sound operating model and organizational alignment

11/9/2020 • 2 minutes to read • [Edit Online](#)

Customer success in cloud adoption efforts often has little to do with technical skills or adoption-related projects. Your operating model creates opportunities to enable adoption or roadblocks that might slow down cloud adoption.

## Alignment

As you drive innovation, alignment between business and technical teams is paramount to the success of your solution.

- For business stakeholders, we've created the [Microsoft AI Business School](#) to support business strategy development and provide example best practices.
- For technical stakeholders, the [Microsoft AI learning paths](#) are available to help you build new AI skills.

## Blockers

When adoption of the cloud is slowed or stalled, it might be wise to evaluate your operating model to enable continued success. When success is inconsistent from workload to workload or project to project, the operating model might be misaligned. If more than one project is stalled by blocking policies, outdated processes, or misalignment of people, the operating model is likely blocking success.

## Opportunities

Beyond the common blockers, a few key opportunities can be scaled across the portfolio through incremental improvements to your operating model. In particular, customers commonly want to scale operational excellence, cost optimization, security, reliability, performance, or people management. Scaling these conversations at the portfolio level can help bring best practices for specific workload-focused teams to all other projects and workloads.

## Get-started guides to enable teams through an operating model

The following guides will help you get started with operating model alignment and improve over time.

GUIDE	DESCRIPTION
<a href="#">How do we deliver operational excellence during cloud transformation?</a>	The steps in this guide will help the strategy team lead organizational change management to consistently ensure operational excellence.
<a href="#">How do we manage enterprise costs?</a>	Start optimizing enterprise costs and manage cost across the environment.
<a href="#">How do we consistently secure the enterprise cloud environment?</a>	This getting started guide can help ensure that the proper security requirements have been applied across the enterprise to minimize risk of breach and accelerate recovery when a breach occurs.

GUIDE	DESCRIPTION
How do we apply the right controls to improve reliability?	This getting started guide helps minimize disruptions related to inconsistencies in configuration, resource organization, security baselines, or resource protection policies.
How do we ensure performance across the enterprise?	This getting started guide can help you establish processes for maintaining performance across the enterprise.
How do we align our organization?	This getting started guide can help you establish an appropriately staffed organizational structure.

## Shared architecture principles

The core principles of a well-managed operating model are based on a set of common architecture principles. The get-started guidance in this article series will help supporting teams as they scale these principles across the cloud platform and throughout the portfolio of workloads.



These principles are shared across Azure Advisor, the Microsoft Azure Well-Architected Framework, and solutions in the Azure Architecture Center:

- [Azure Advisor](#) evaluates the principles for individual assets across solutions, workloads, and the full portfolio.
- [Azure Architecture Center](#) applies these principles to develop and manage specific technical solutions.
- [Microsoft Azure Well-Architected Framework](#) helps balance these principles across a workload, to guide

architecture decisions.

- [Cloud Adoption Framework](#) ensures that the principles scale across the portfolio to enable adoption teams through a well-managed environment.

# Get started: Deliver operational excellence during digital transformation

11/9/2020 • 5 minutes to read • [Edit Online](#)

How do you ensure operational excellence during digital transformation? Operational excellence is a business function that directly affects IT decisions. To achieve operational excellence, you must focus on customer and stakeholder value by keeping an eye on revenue, risk, and cost impacts.

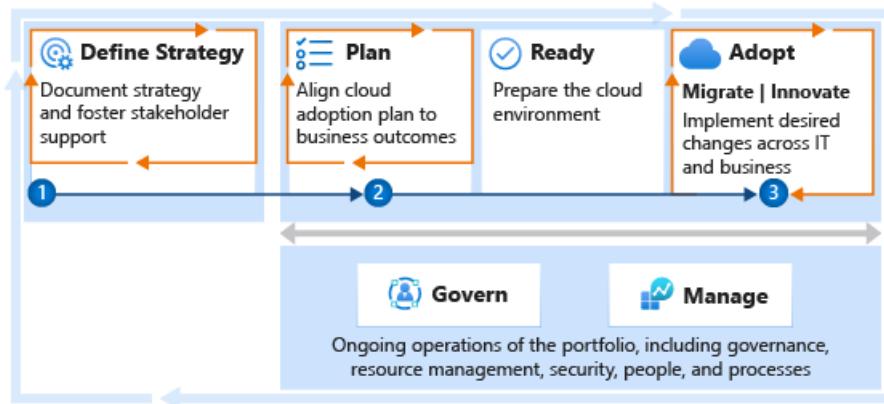
This organizational change management approach requires:

- A defined strategy.
- Clear business outcomes.
- Change management planning.

From a cloud perspective, you can manage the impact of risk and cost by making post-adoption changes and continuously refining operational processes. Areas to monitor include systems automation, IT operations management practices, and Resource Consistency discipline throughout the cloud adoption lifecycle.

The steps in this article can help the strategy team lead the organizational change management that's required to consistently ensure operational excellence.

Operational excellence across the enterprise and portfolio starts with peer processes of strategy and planning to align and report on organizational change management expectations. The following steps help technical teams deliver the disciplines required to achieve operational excellence.



## Step 1: Define a strategy to guide digital transformation and operational excellence expectations

A clear business strategy is the foundation for any digital transformation and operational excellence effort. IT can reduce costs and streamline IT processes. Without a clear strategy, it's difficult to understand how those changes might affect the business outcomes identified in the broader transformation effort.

### Deliverables:

- Record motivations, outcomes, and business justification in the [strategy and plan template](#).
- Ensure learning metrics are well understood and included in the business outcomes section. Those metrics guide operational excellence activities and reporting within IT.

### Guidance to support deliverable completion:

- **Understand motivations:** Critical business events and some migration motivations tend to be cost sensitive. These areas can increase the importance of cost control for all later efforts. Other forward-looking motivations related to innovation or growth through migration might be focused more on top-line revenue. Understanding motivations helps you prioritize your cost management.
- **Business outcomes:** Some fiscal outcomes tend to be extremely cost sensitive. When the desired outcomes map to fiscal metrics, you should invest early in the Cost Management governance discipline.
- **Business justification:** The business justification serves as a high-level view of the overall financial plan for cloud adoption. It can be a good source for initial budgeting efforts.
- **Learning metrics:** To maintain alignment between the overarching business strategy and the more tactical change-management plans, establish learning metrics. These metrics should be designed to show iterative and incremental progress toward the plan.

ACCOUNTABLE TEAM	RESPONSIBLE AND SUPPORTING TEAMS
<ul style="list-style-type: none"> <li>• Cloud strategy team</li> </ul>	<ul style="list-style-type: none"> <li>• Cloud adoption team</li> <li>• Cloud governance team</li> <li>• Cloud operations team</li> <li>• Cloud center of excellence or central IT team</li> </ul>

## Step 2: Develop an organizational change management plan to span cloud adoption

Organizational change management is an iterative approach to subtly realign people, processes, and technology to support a holistic business strategy. In the case of operational excellence for digital transformation, this approach often centers on an IT-centric cloud adoption plan.

### Deliverables:

- Update the [strategy and plan template](#) to reflect change that's needed to achieve the desired strategy. The changes recorded can include:
  - An assessment of the existing digital estate.
  - A cloud adoption plan that reflects the required changes and the work involved.
  - The organizational changes that are required to deliver on the plan.
  - A plan for addressing the skills that are needed to enable the existing team to successfully complete the required work.

### Guidance to support deliverable completion:

- [Gather inventory:](#) Establish a source of data for analysis of the digital estate prior to adoption.
- [Best practice: Azure Migrate:](#) Use Azure Migrate to gather inventory.
- [Incremental rationalization:](#) During incremental rationalization, a quantitative analysis identifies cloud candidates for budgeting purposes.
- [Align cost models and forecast models:](#) Use Azure Cost Management + Billing to align cost and forecast models by [creating budgets](#).
- [Build your cloud adoption plan:](#) Build a plan with actionable workload, assets, and timeline details.

ACCOUNTABLE TEAM	RESPONSIBLE AND SUPPORTING TEAMS
------------------	----------------------------------

ACCOUNTABLE TEAM	RESPONSIBLE AND SUPPORTING TEAMS
<ul style="list-style-type: none"> <li>Cloud strategy team</li> </ul>	<ul style="list-style-type: none"> <li>Cloud adoption team</li> <li>Cloud governance team</li> <li>Cloud operations team</li> <li>Cloud center of excellence or central IT team</li> </ul>

## Step 3: Manage change across cloud adoption efforts

Realization of business outcomes is the result of continuous delivery of adoption waves. Those waves could include migration and innovation cycles. In either case, delivery on operational excellence starts with regular cycles of change management.

Each wave (or release, in agile terms) delivers a set of workloads to the cloud. As each wave of adoption is completed, the cloud strategy team reports on progress toward learning metrics, business outcomes, and the overall strategy. Likewise, as each wave of adoption is completed, the adoption teams need backlog updates that reflect the prioritized workloads in the plan. These updates are based on any changes to business plans and customer needs.

### Deliverables:

- Continuous testing and improvements to the strategy and change management plan based on changing market conditions and completion of the most recent wave of technical change.

### Guidance to support deliverable completion:

- [Release planning](#): Approaches to change management through release planning.
- [Incremental rationalization](#): Iterative approach to change management. The focus is on managing the release backlog to support manageable waves of change.
- [Power of 10 approach](#): Limits the change management plan. The focus is on detailed analysis and planning of a continuous base of 10 workloads to balance incremental change and iterative adoption efforts.
- [Align iteration paths](#): Update and add details at each release to ensure current iteration paths.
- [Assess workloads](#): The efforts of the cloud adoption team to evaluate and act on the most recent set of migration priorities.
- [Business value consensus](#): The cloud adoption team's efforts to ensure business value alignment at each release of new innovation.

ACCOUNTABLE TEAM	RESPONSIBLE AND SUPPORTING TEAMS
<ul style="list-style-type: none"> <li>Cloud strategy team</li> </ul>	<ul style="list-style-type: none"> <li>Cloud adoption team</li> </ul>

## Value statement

The previous steps outline a business-led approach to establish operational excellence requirements throughout digital transformation. This approach provides a consistent foundation that carries through other operating model functions.



## Next steps to delivering operational excellence across the portfolio

Operational excellence requires a disciplined approach to reliability, performance, security, and cost optimization. Use the remaining guidance in this series to implement these principles through consistent approaches to automation.

- **Cost optimization:** Continuously optimize operating costs by using the getting started guide on [managing enterprise costs](#)
- **Security:** Reduce risk by integrating enterprise security across the portfolio by using the getting started guide on [implementing security across the portfolio](#).
- **Performance management:** Ensure IT asset performance supports business processes by using the getting started guide on [performance management across the enterprise](#).
- **Reliability:** Improve reliability and reduce business disruptions by using the getting started guide on [implementing controls to create reliability](#).

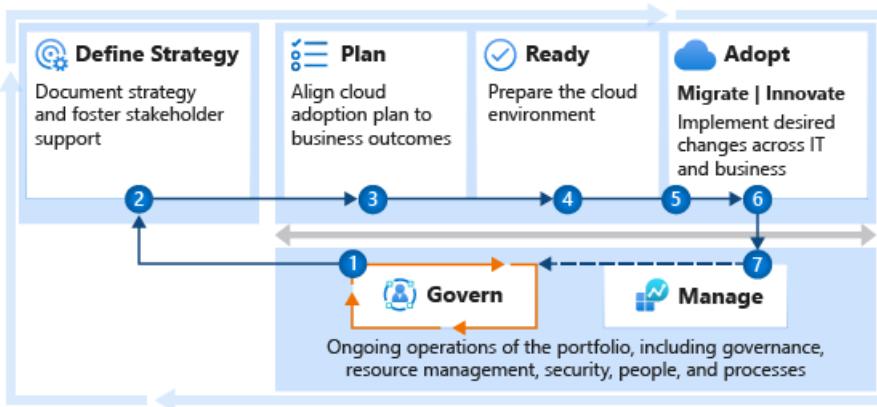
# Get started: Manage cloud costs

11/9/2020 • 8 minutes to read • [Edit Online](#)

The Cost Management discipline of cloud governance focuses on establishing budgets, monitoring cost allocation patterns, and implementing controls to improve cloud spending behaviors across the IT portfolio. Enterprise cost optimization involves many other roles and functions to minimize cost and balance the demands of scale, performance, security, and reliability. This article maps those various supporting functions into a getting started guide that helps create alignment among the involved teams.

However, enterprise cost optimization involves many other roles and functions to minimize cost and balance the demands of scale, performance, security, and reliability. This article maps those supporting functions to help create alignment between the involved teams.

Governance is the cornerstone of cost optimization within any large enterprise. The following section outlines cost optimization guidance within the context of governance. The subsequent steps help each team take actions that target its role in cost optimization. Together, these steps will help your organization get started on a journey toward cost optimization.



## Step 1: Optimize enterprise costs

The cloud governance team is well prepared to evaluate and act on overspending or unplanned spending through a combination of monitoring performance, reducing resource sizing, and safely terminating unused resources. Enterprise cost optimization starts with a shared team understanding of the tools, processes, and dependencies required to wisely act on cost concerns at an environment level.

### Deliverables:

- Implement wise changes to your Cost Management policies across the enterprise.
- Document your Cost Management policies, processes, and design guidance in the [Cost Management discipline template](#).

These deliverables are the result of a few recurring tasks:

- Ensure strategic alignment with the cloud strategy team (which includes workload stakeholders across the portfolio).
- Optimize cost across the environment:
  - Manually or automatically shut down unused VMs.
  - Delete or deallocate stopped VMs.
  - Ensure proper resource sizing.

- Align spending to budget expectations.
- Validate any architectural change by using the Microsoft Azure Well-Architected Review to facilitate a conversation with technical owners of the workloads.

#### Guidance to support deliverable completion:

- Ensure that all workloads and resources follow [proper naming and tagging conventions](#). Enforce tagging conventions by using [Azure Policy](#) with a specific emphasis on tags for "cost center" and "technical owner."
- On a regular basis, review and apply [Cost Management discipline best practices](#) to guide analysis and improvements across the enterprise. Important governance practices include:
  - Acting on [general cost best practices](#) to reduce sizing and costs and to stop unused machines.
  - Applying [hybrid use benefits](#) to reduce licensing costs.
  - Aligning [reserved instances](#) to reduce resource costs.
  - [Monitoring resource utilization](#) to minimize impacts on resource performance.
  - [Reducing nonproduction costs](#) through policies to govern nonproduction environments.
  - Acting on [cost optimization recommendations](#).
- Trade-offs at the workload level might be needed to implement effective cost optimization changes. The [Microsoft Azure Well-Architected Framework](#) and [Microsoft Azure Well-Architected Review](#) can help guide those conversations with the technical owner of a specific workload.
- If you're new to cloud governance, establish [governance policies, processes, and disciplines](#) using the [Govern](#) methodology.
- If you're new to the Cost Management discipline, consider following the [Cost Management discipline improvements article](#), with a focus on the [implementation](#) section.

ACCOUNTABLE TEAM	RESPONSIBLE AND SUPPORTING TEAMS
<ul style="list-style-type: none"> <li>● Cloud governance team</li> </ul>	<ul style="list-style-type: none"> <li>● Cloud strategy team</li> <li>● Cloud adoption team</li> <li>● Cloud center of excellence or central IT team</li> </ul>

The governance team can detect and drive significant cost optimization across most enterprises. Basic, data-driven resource sizing can have an immediate and measurable impact on costs.

As discussed in [Build a cost-conscious organization](#), an enterprise-wide focus on cost management and cost optimization can deliver much more value. The following steps demonstrate ways the various teams can help build a cost-conscious organization.

## Step 2: Define a strategy

Strategic decisions directly affect cost controls, rippling through the adoption lifecycle and into long-term operations. Strategic clarity will improve cost optimization efforts, driven by the governance team.

#### Deliverables:

- Record motivations, outcomes, and business justification in the [strategy and plan template](#).
- Create your first budget by using Azure Cost Management + Billing.

#### Guidance to support deliverable completion:

- [Understand motivations](#). Critical business events and some migration motivations tend to be cost sensitive, increasing the importance of cost control for all later efforts. Other forward-looking motivations related to

innovation or growth through migration might focus more on top-line revenue. Understanding motivations will help you decide how high to prioritize your cost management.

- **Business outcomes.** Some fiscal outcomes tend to be extremely cost-sensitive. When the desired outcomes map to fiscal metrics, you should invest in the Cost Management governance discipline very early.
- **Business justification.** The business justification serves as a high-level view of the financial plan for cloud adoption. This is a good source for initial budgeting efforts.

ACCOUNTABLE TEAM	RESPONSIBLE AND SUPPORTING TEAMS
<ul style="list-style-type: none"><li>• Cloud strategy team</li></ul>	<ul style="list-style-type: none"><li>• Cloud governance team</li><li>• Cloud adoption team</li><li>• Cloud center of excellence or central IT team</li></ul>

## Step 3: Develop a cloud adoption plan

The adoption plan provides clarity on the timeline of activities during adoption. Aligning the plan and the digital estate analysis allows you to forecast your monthly growth in spending. It also helps your cloud governance team align processes and identify spending patterns.

### Deliverables:

- Complete steps 1 through 6 of building a [cloud adoption plan](#).
- Work with your cloud governance team to refine budgets and create realistic spending forecasts.

### Guidance to support deliverable completion:

- [Gather inventory](#). Establish a source of data for analysis of the digital estate before adoption.
- [Best practice: Azure Migrate](#). Use Azure Migrate to gather inventory.
- [Incremental rationalization](#). During incremental rationalization and quantitative analysis, identify cloud candidates for budgeting purposes.
- [Align cost models and forecast models](#). Use Azure Cost Management + Billing to align cost and forecast models by [creating budgets](#).
- [Build your cloud adoption plan](#). Build a plan with actionable workload, assets, and timeline details. This plan provides the basis for spending over time (or cost forecasting). *Spending over time* is the initial baseline for all actionable optimization analysis within the Cost Management governance discipline.

ACCOUNTABLE TEAM	RESPONSIBLE AND SUPPORTING TEAMS
<ul style="list-style-type: none"><li>• Cloud adoption team</li></ul>	<ul style="list-style-type: none"><li>• Cloud strategy team</li><li>• Cloud governance team</li><li>• Cloud center of excellence or central IT team</li></ul>

## Step 4: Implement best practices for landing zones

The Ready methodology of the Microsoft Cloud Adoption Framework for Azure focuses heavily on the development of landing zones to host workloads in the cloud. During implementation of landing zones, an organization should consider various decisions for cost optimization.

### Deliverables:

- Deploy one or more landing zones that can host workloads in the short-term adoption plan.

- Ensure that all landing zones meet cost optimization decisions and cost management requirements.

#### Guidance to support deliverable completion:

- [Track costs](#). Establish a well-managed environment hierarchy, provide the right level of cost access, and use additional cost management resources in each landing zone.
- [Optimize your cloud investment](#). Understand best practices for optimizing investments.
- [Create and manage budgets](#). Understand best practices for creating and managing budgets.
- [Optimize costs from recommendations](#). Understand best practices for using recommendations that will optimize costs.
- [Monitor usage and spending](#). Understand best practices for monitoring usage and spending within a landing zone.

ACCOUNTABLE TEAM	RESPONSIBLE AND SUPPORTING TEAMS
<ul style="list-style-type: none"> <li>Cloud adoption team</li> </ul>	<ul style="list-style-type: none"> <li>Cloud strategy team</li> <li>Cloud governance team</li> <li>Cloud center of excellence or central IT team</li> </ul>

## Step 5: Complete waves of migration effort

Migration is a repeatable process executed by the cloud adoption team. Throughout this process, there are many opportunities to optimize costs across your portfolio. Many of these in-process decisions are applied to a small group of workloads during each migration wave or iteration.

#### Deliverables:

- Benchmark, test, resize, and deploy a collection of fully optimized workloads.

#### Guidance to support deliverable completion:

- [Migration-focused cost-control mechanisms](#) provides insights about the cloud-native cost optimization controls that help during migration.
- [Best practices for optimizing cost of migrated workloads](#) contains a checklist of 14 best practices to follow before and after migration to maximize cost optimization of each workload release.

Long-term operational costs are a common theme in each area of migration process improvements. This list of process improvements is organized by the phase of the migration process:

- [Prerequisites](#) provides information on managing change and the backlog, which influences both budgeted and actual cloud costs.
- [Assess](#) provides six specific processes, from validating assumptions to understanding partner options. Each process influences cloud optimization opportunities.
- [Migrate](#) contains one process suggestion about remediating assets. This suggestion provides an opportunity to optimize the as-configured state, in favor of an optimized solution.
- [Promote](#) focuses heavily on testing, resizing, validating, and releasing migrated assets, along with decommissioning retired assets. This is the first clear point at which forecasts and budgets can be tested against actual performance and configuration.

ACCOUNTABLE TEAM	RESPONSIBLE AND SUPPORTING TEAMS
<ul style="list-style-type: none"> <li>Cloud adoption team</li> </ul>	<ul style="list-style-type: none"> <li>Cloud strategy team</li> <li>Cloud governance team</li> <li>Cloud center of excellence or central IT team</li> </ul>

## Step 6: Drive customer-focused innovation

Innovation and development of new products require a much deeper degree of architectural review. The Cloud Adoption Framework provides details on the innovation process and product management thinking. Cost optimization decisions about innovations are largely out of scope in this guidance.

### Deliverables:

- Make key architectural decisions about innovations to balance cost and other critical design considerations.

### Guidance to support deliverable completion:

- Use the [Microsoft Azure Well-Architected Review](#) to understand the balance in architecture decisions.
- Review the [Microsoft Azure Well-Architected Framework](#) for deeper guidance on cost optimization during innovation.

ACCOUNTABLE TEAM	RESPONSIBLE AND SUPPORTING TEAMS
<ul style="list-style-type: none"> <li>Cloud adoption team</li> </ul>	<ul style="list-style-type: none"> <li>Cloud strategy team</li> <li>Cloud governance team</li> <li>Cloud center of excellence or central IT team</li> </ul>

## Step 7: Implement sound operations

Establishing a solid management baseline will help you collect data and create operational alerts. This effort can aid in detecting opportunities to optimize costs. It will create a balance between resiliency and cost optimization.

### Deliverables:

- Monitor your enterprise environment for ongoing recommendations to optimize costs, aligned to the criticality and resiliency classifications of each workload.

### Guidance to support deliverable completion:

- [Create business alignment](#) to gain clarity regarding criticality and appetite for resiliency investments.

ACCOUNTABLE TEAM	RESPONSIBLE AND SUPPORTING TEAMS
<ul style="list-style-type: none"> <li>Cloud operations team</li> </ul>	<ul style="list-style-type: none"> <li>Cloud strategy team</li> <li>Cloud governance team</li> <li>Cloud center of excellence or central IT team</li> </ul>

## Value statement

Following these steps helps you [build a cost-conscious organization](#). Simplify cost optimization by using shared ownership and driving collaboration with the right teams at the right times.

# Get started: Implement security across the enterprise environment

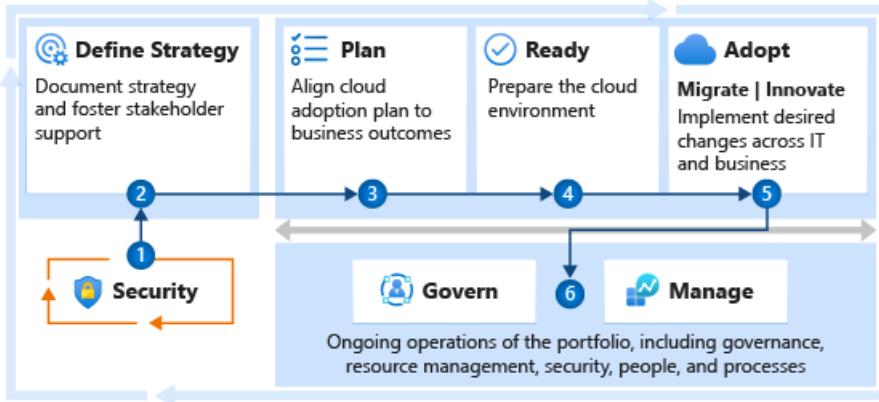
11/9/2020 • 13 minutes to read • [Edit Online](#)

Security helps create assurances of confidentiality, integrity, and availability for a business. Security efforts have a critical focus on protecting against the potential impact to operations caused by both internal and external malicious and unintentional acts.

This getting started guide outlines the key steps that will mitigate or avoid the business risk from cybersecurity attacks. It can help you rapidly establish essential security practices in the cloud and integrate security into your cloud adoption process.

The steps in this guide are intended for all roles that support security assurances for cloud environments and landing zones. Tasks include immediate risk mitigation priorities, guidance on building a modern security strategy, operationalizing the approach, and executing on that strategy.

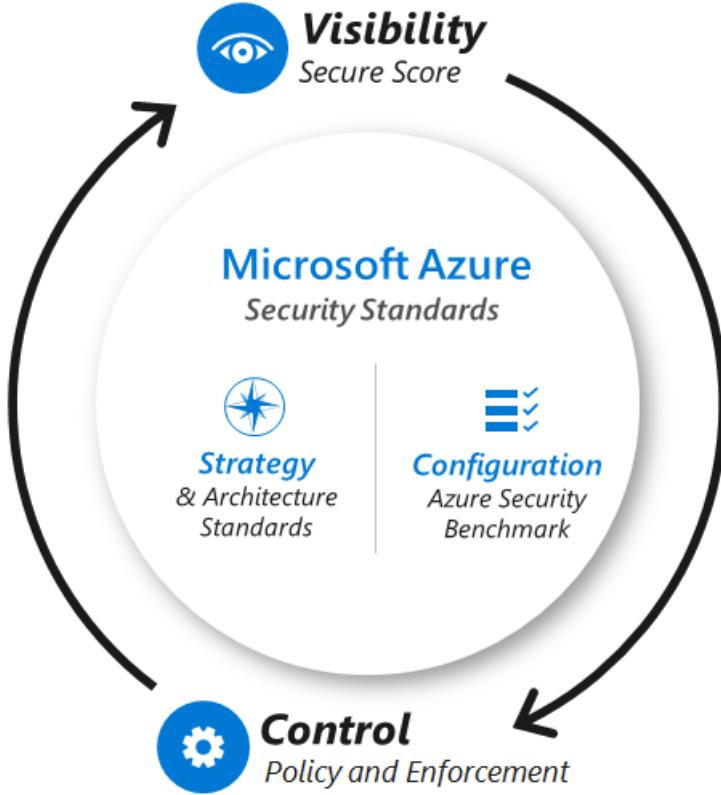
This guide includes elements from across the Microsoft Cloud Adoption Framework for Azure:



Adhering to the steps in this guide will help you integrate security at critical points in the process. The goal is to avoid obstacles in cloud adoption and reduce unnecessary business or operational disruption.

Microsoft has built capabilities and resources to help accelerate your implementation of this security guidance on Microsoft Azure. You'll see these resources referenced throughout this guide. They're designed to help you establish, monitor, and enforce security, and they're frequently updated and reviewed.

The following diagram shows a holistic approach for using security guidance and platform tooling to establish security visibility and control over your cloud assets in Azure. We recommend this approach.



Use these steps to plan and execute your strategy for securing your cloud assets and using the cloud to modernize security operations.

## Step 1: Establish essential security practices

Security in the cloud starts with applying the most important security practices to the people, process, and technology elements of your system. Additionally, some architectural decisions are foundational and are very difficult to change later so should be carefully applied.

Whether you're already operating in the cloud or you're planning for future adoption, we recommend that you follow these 11 essential security practices (in addition to meeting any explicit regulatory compliance requirements).

### People:

1. [Educate teams about the cloud security journey](#)
2. [Educate teams on cloud security technology](#)

### Process:

3. [Assign accountability for cloud security decisions](#)
4. [Update Incident Response \(IR\) processes for cloud](#)
5. [Establish security posture management](#)

### Technology:

6. [Require Passwordless or Multi-Factor Authentication \(MFA\)](#)
7. [Integrate native firewall and network security](#)
8. [Integrate native threat detection](#)

### Foundational Architecture Decisions:

9. Standardize on a single directory and identity
10. Use identity based access control (instead of keys)
11. Establish a single unified security strategy

#### NOTE

Each organization should define its own minimum standards. Risk posture and subsequent tolerance to that risk can vary widely based on industry, culture, and other factors. For example, a bank might not tolerate any potential damage to its reputation from even a minor attack on a test system. Some organizations would gladly accept that same risk if it accelerated their digital transformation by three to six months.

## Step 2: Modernize the security strategy

Effective security in the cloud requires a strategy that reflects the current threat environment and the nature of the cloud platform that's hosting the enterprise assets. A clear strategy improves the effort of all teams to provide a secure and sustainable enterprise cloud environment. The security strategy must enable defined business outcomes, reduce risk to an acceptable level, and enable employees to be productive.

A cloud security strategy provides guidance to all teams working on the technology, processes, and people readiness for this adoption. The strategy should inform the cloud architecture and technical capabilities, guide the security architecture and capabilities, and influence the training and education of teams.

#### Deliverables:

The strategy step should result in a document that can easily be communicated to many stakeholders within the organization. The stakeholders can potentially include executives on the organization's leadership team.

We recommended capturing the strategy in a presentation to facilitate easy discussion and updating. This presentation can be supported with a document, depending on the culture and preferences.

- **Strategy presentation:** You might have a single strategy presentation, or you might choose to also create summary versions for leadership audiences.
  - **Full presentation:** This should include the full set of elements for the security strategy in the main presentation or in optional reference slides.
  - **Executive summaries:** Versions to use with senior executives and board members might contain only critical elements relevant to their role, such as risk appetite, top priorities, or accepted risks.
- You can also record motivations, outcomes, and business justifications in the [strategy and plan template](#).

#### Best practices for building security strategy:

Successful programs incorporate these elements into their security strategy process:

- **Align closely to business strategy:** Security's charter is to protect business value. It's critical to align all security efforts to that purpose and minimize internal conflict.
  - **Build a shared understanding** of business, IT, and security requirements.
  - **Integrate security early into cloud adoption** to avoid last-minute crises from avoidable risks.
  - **Use an agile approach** to immediately establish minimum security requirements and continuously improve security assurances over time.
  - **Encourage security culture change** through intentional proactive leadership actions.

For more information, see [Transformations, mindsets, and expectations](#).

- **Modernize security strategy:** The security strategy should include considerations for all aspects of modern technology environment, current threat landscape, and security community resources.

- Adapt to the shared responsibility model of the cloud.
- Include all cloud types and multicloud deployments.
- Prefer native cloud controls to avoid unnecessary and harmful friction.
- Integrate the security community to keep up with the pace of attacker evolution.

#### Related resources for additional context:

- [Evolution of threat environment, roles, and digital strategies](#)
- [Transformation of security, strategies, tools, and threats](#)
- Strategy considerations for the Cloud Adoption Framework:
  - [Modernize your security strategy](#)
  - [Cybersecurity resilience](#)
  - [How cloud is changing security relationships and responsibilities](#)

ACCOUNTABLE TEAM	RESPONSIBLE AND SUPPORTING TEAMS
<ul style="list-style-type: none"> <li>● Security leadership team (chief information security officer (CISO) or equivalent)</li> </ul>	<ul style="list-style-type: none"> <li>● Cloud strategy team</li> <li>● Cloud security team</li> <li>● Cloud adoption team</li> <li>● Cloud center of excellence or central IT team</li> </ul>

#### Strategy approval:

Executives and business leaders with accountability for outcomes or risks of business lines within the organization should approve this strategy. This group might include the board of directors, depending on the organization.

## Step 3: Develop a security plan

Planning puts the security strategy into action by defining outcomes, milestones, timelines, and task owners. This plan also outlines the roles and responsibilities of the teams.

Security planning and cloud adoption planning should not be done in isolation. It's critical to invite the cloud security team into the planning cycles early, to avoid work stoppage or increased risk from security issues being discovered too late. Security planning works best with in-depth knowledge and awareness of the digital estate and existing IT portfolio that comes from being fully integrated into the cloud planning process.

#### Deliverables:

- **Security plan:** A security plan should be part of the main planning documentation for the cloud. It might be a document that uses the [strategy and plan template](#), a detailed slide deck, or a project file. Or it might be a combination of these formats, depending on the organization's size, culture, and standard practices.

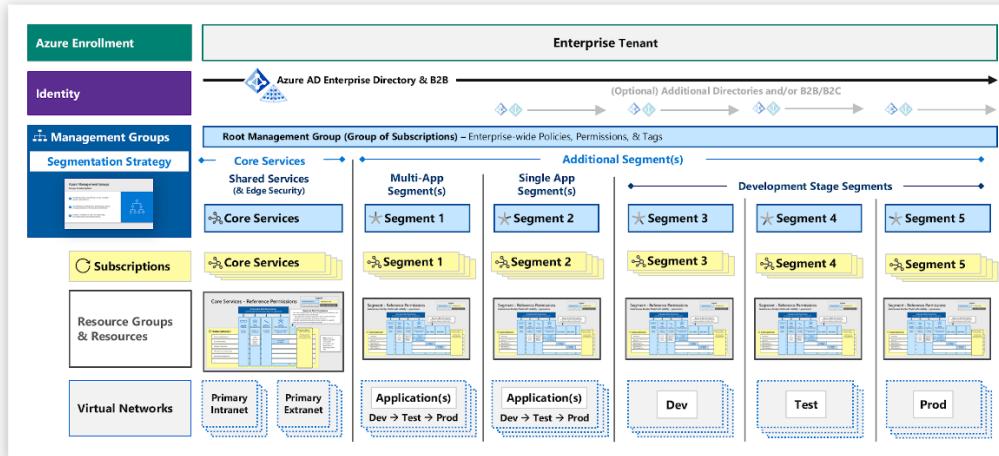
The security plan should include all of these elements:

- **Organizational functions plan**, so teams know how current security roles and responsibilities will change with the move to the cloud.
- **Security skills plan** to support team members as they navigate the significant changes in technology, roles, and responsibilities.
- **Technical security architecture and capabilities roadmap** to guide technical teams.

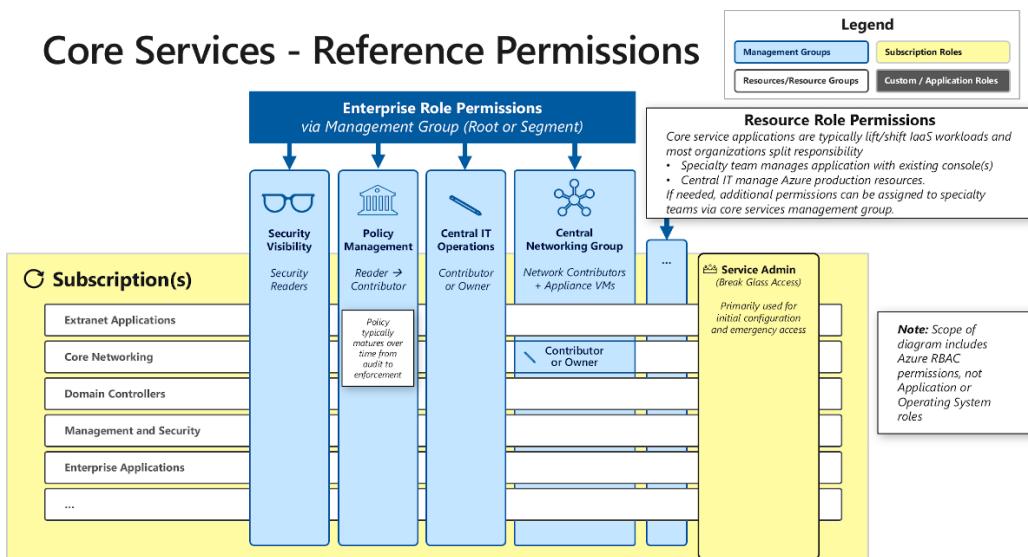
Microsoft provides reference architectures and technology capabilities to help you as you build your architecture and roadmap, including:

- Azure components and reference model to accelerate planning and design of Azure security roles.

## Reference Design - Azure Administration Model



## Core Services - Reference Permissions



- Microsoft cybersecurity reference architecture to build a cybersecurity architecture for a hybrid enterprise that spans on-premises and cloud resources.
- Security operations center (SOC) reference architecture to modernize security detection, response, and recovery.
- Zero-trust user access reference architecture to modernize access control architecture for cloud generation.
- Azure Security Center and Microsoft cloud application security to help secure cloud assets.
- Security awareness and education plan, so all teams have basic critical security knowledge.
- Asset sensitivity marking to designate sensitive assets by using a taxonomy aligned to business impact. The taxonomy is built jointly by business stakeholders, security teams, and other interested parties.
- Security changes to the cloud plan: Update other sections of the cloud adoption plan to reflect changes triggered by the security plan.

### Best practices for security planning:

Your security plan is likely to be more successful if your planning takes the approach of:

- Assume a hybrid environment: That includes software as a service (SaaS) applications and on-premises

environments. It also includes multiple cloud infrastructure as a service (IaaS) and platform as a service (PaaS) providers, if applicable.

- **Adopt agile security:** Establish minimum security requirements first and move all noncritical items to a prioritized list of next steps. This should not be a traditional, detailed plan of 3-5 years. The cloud and threat environment change too fast to make that type of plan useful. Your plan should focus on developing the beginning steps and end state:
  - **Quick wins** for the immediate future that will deliver a high impact before longer-term initiatives begin. The time frame can be 3-12 months, depending on organizational culture, standard practices, and other factors.
  - **Clear vision** of the desired end state to guide each team's planning process (which might take multiple years to achieve).
- **Share the plan broadly:** Increase awareness of, feedback from, and buy-in by stakeholders.
- **Meet the strategic outcomes:** Ensure that your plan aligns to and accomplishes the strategic outcomes described in the security strategy.
- **Set ownership, accountability, and deadlines:** Ensure that the owners for each task are identified and are committed to completing that task in a specific time frame.
- **Connect with the human side of security:** Engage people during this period of transformation and new expectations by:
  - **Actively supporting team member transformation** with clear communication and coaching on:
    - What skills they need to learn.
    - Why they need to learn the skills (and the benefits of doing so).
    - How to get this knowledge (and provide resources to help them learn).
  - **Making security awareness engaging** to help people genuinely connect with their part of keeping the organization safe.
- **Review Microsoft learnings and guidance:** Microsoft has published insights and perspectives to help your organization plan its transformation to the cloud and a modern security strategy. The material includes recorded training, documentation, and security best practices and recommended standards.

For technical guidance to help build your plan and architecture, see the [Microsoft security documentation](#).

ACCOUNTABLE TEAM	RESPONSIBLE AND SUPPORTING TEAMS
<ul style="list-style-type: none"><li>● Cloud security team</li></ul>	<ul style="list-style-type: none"><li>● Cloud strategy team</li><li>● Cloud governance team</li><li>● Any risk teams in your organization</li><li>● Cloud center of excellence or central IT team</li></ul>

#### Security plan approval:

The security leadership team (CISO or equivalent) should approve the plan.

## Step 4: Secure new workloads

It's a lot easier to start in a secure state than to retrofit security later into your environment. We strongly recommend starting with a secure configuration to ensure that workloads are migrated to, and developed and

tested in, a secure environment.

During [landing zone](#) implementation, many decisions can affect security and risk profiles. The cloud security team should review the landing zone configuration to ensure that it meets the security standards and requirements in your organization's security baselines.

#### Deliverables:

- Ensure that new landing zones meet the organization's compliance and security requirements.

#### Guidance to support deliverable completion:

- **Blend existing requirements and cloud recommendations:** Start with recommended guidance and then adapt this to your unique security requirements. We have seen challenges with trying to enforce existing on-premises policies and standards, because these often refer to outdated technology or security approaches.

Microsoft has published guidance to help you build your security baselines:

- [Azure security standards for strategy and architecture](#): Strategy and architectural recommendations to shape your environment's security posture.
- [Azure security benchmarks](#): Specific configuration recommendations for securing Azure environments.
- [Azure security baseline training](#).
- **Provide guardrails:** Safeguards should include automated policy auditing and enforcement. For these new environments, teams should strive to both audit and enforce the organization's security baselines. These efforts can help minimize security surprises during the development of workloads, as well as continuous integration and continuous deployment (CI/CD) of workloads.

Microsoft provides several native capabilities in Azure to enable this:

- [Secure score](#): Use a scored assessment of your Azure security posture to track security efforts and projects in your organization.
- [Azure Blueprints](#): Cloud architects and centralized IT groups can define a repeatable set of Azure resources that implements and adheres to an organization's standards, patterns, and requirements.
- [Azure Policy](#): This is the foundation of the visibility and control capabilities that the other services use. Azure Policy is integrated into [Azure Resource Manager](#), so you can audit changes and enforce policies across any resource in Azure before, during, or after its creation.
- [Improve landing zone operations](#): Use best practices for improving security within a landing zone.

ACCOUNTABLE TEAM	RESPONSIBLE AND SUPPORTING TEAMS
<ul style="list-style-type: none"><li>• Cloud security team</li></ul>	<ul style="list-style-type: none"><li>• Cloud adoption team</li><li>• Cloud platform team</li><li>• Cloud strategy team</li><li>• Cloud governance team</li><li>• Cloud center of excellence or central IT team</li></ul>

## Step 5: Secure existing cloud workloads

Many organizations have already deployed assets to enterprise cloud environments without applying the security best practices, creating increased business risk.

After you ensure that new applications and landing zones follow security best practices, you should focus on bringing existing environments up to the same standards.

## Deliverables:

- Ensure that all existing cloud environments and landing zones meet the organization's compliance and security requirements.
- Test operational readiness of production deployments by using policies for security baselines.
- Validate adherence to design guidance and security requirements for security baselines.

## Guidance to support deliverable completion:

- Use the same security baselines that you built in [Step 4](#) as your ideal state. You might have to adjust some policy settings to only audit instead of enforcing them.
- Balance operational and security risk. Because these environments might host production systems that enable critical business processes, you might need to implement security improvements incrementally to avoid risking operational downtime.
- Prioritize the discovery and remediation of security risk by business criticality. Start with workloads that have a high business impact if compromised and workloads that have a high exposure to risk.

For more information, see [Identify and classify business-critical applications](#).

ACCOUNTABLE TEAM	RESPONSIBLE AND SUPPORTING TEAMS
<ul style="list-style-type: none"><li>• Cloud adoption team</li></ul>	<ul style="list-style-type: none"><li>• Cloud adoption team</li><li>• Cloud strategy team</li><li>• Cloud security team</li><li>• Cloud governance team</li><li>• Cloud center of excellence or central IT team</li></ul>

## Step 6: Govern to manage and improve security posture

Like all modern disciplines, security is an iterative process that should focus on continuous improvement. Security posture can also decay if organizations don't sustain focus on it over time.

Consistent application of security requirements comes from sound governance disciplines and automated solutions. After the cloud security team defines the security baselines, those requirements should be audited to ensure they're applied consistently to all cloud environments (and enforced where applicable).

## Deliverables:

- Ensure that the organization's security baselines are applied to all relevant systems. Audit anomalies by using a [secure score](#) or a similar mechanism.
- Document your Security Baseline policies, processes, and design guidance in the [Security Baseline discipline template](#).

## Guidance to support deliverable completion:

- Use the same security baselines and auditing mechanisms that you built in [Step 4](#) as technical components of monitoring the baselines. Complement these baselines with people and process controls to ensure consistency.
- Ensure that all workloads and resources follow proper [naming and tagging conventions](#). [Enforce tagging conventions by using Azure Policy](#), with a specific emphasis on tags for "data sensitivity."
- If you're new to cloud governance, establish [governance policies, processes, and disciplines](#) by using the Govern methodology.

ACCOUNTABLE TEAM	RESPONSIBLE AND SUPPORTING TEAMS
<ul style="list-style-type: none"><li>Cloud governance team</li></ul>	<ul style="list-style-type: none"><li>Cloud strategy team</li><li>Cloud security team</li><li>Cloud center of excellence or central IT team</li></ul>

## Next steps

The steps in this guide have helped you implement the strategy, controls, processes, skills, and culture needed to consistently manage security risks across the enterprise.

As you continue into the operations mode of cloud security, consider these next steps:

- Review [Microsoft security documentation](#). It provides technical guidance to help security professionals build and improve cybersecurity strategy, architecture, and prioritized roadmaps.
- Review security information in [Built-in security controls for Azure services](#).
- Review Azure security tools and services in [Security services and technologies available on Azure](#).
- Review the [Microsoft Trust Center](#). It contains extensive guidance, reports, and related documentation that can help you perform risk assessments as part of your regulatory compliance processes.
- Review third-party tools available to facilitate meeting your security requirements. For more information, see [Integrate security solutions in Azure Security Center](#).

# Get started: Improve reliability with the right controls

11/9/2020 • 7 minutes to read • [Edit Online](#)

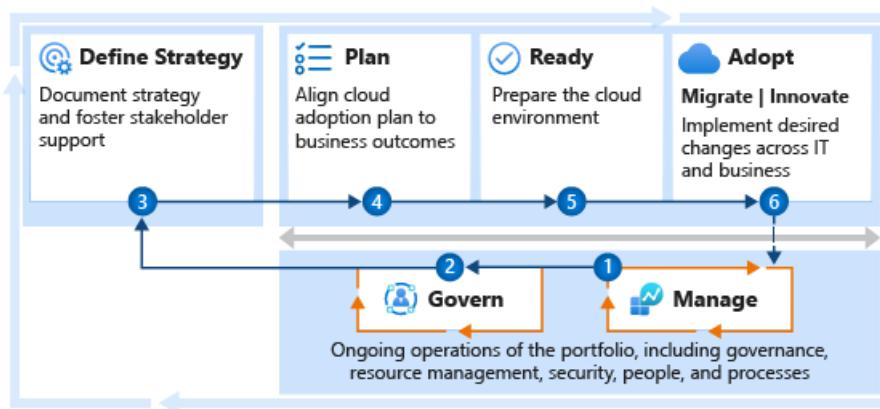
How do you apply the right controls to improve reliability? This article helps you minimize disruptions related to:

- Inconsistencies in configuration.
- Resource organization.
- Security baselines.
- Resource protection.

The steps in this article help the operations team balance reliability and cost across the IT portfolio. This article also helps the governance team to ensure that balance is applied consistently. Reliability also depends on other roles and functions. This article maps supporting functions to help you create alignment among the involved teams.

Operations management and governance are equal partners in enterprise reliability. The decisions you make about operational practices set the baseline for reliability. The approaches used to govern the overall environment ensure consistency across all resources.

The first two steps in this article help both teams get started. They're listed sequentially, but you can perform them in parallel. The subsequent steps help you get the entire enterprise started on a shared journey toward more reliable solutions throughout the enterprise.



## Step 1: Establish operations management requirements

Not all workloads are created equal. In any environment, there are workloads that have a direct and constant impact on the business. There are also supporting business processes and workloads that have a smaller impact on the overall business. In this step, the cloud operations team identifies and implements initial requirements to support the overall IT portfolio.

### Deliverables:

- Implement a management baseline to define the standard operations that are required for all production workloads.
- Negotiate business commitments with the cloud strategy team to develop a plan for advanced operations and resiliency requirements.
- Expand your management baseline, if additional operations are required for the majority of workloads.
- Apply advanced operations requirements to landing zones and resources that support the workloads that are most critical.
- Document operations decisions across the IT portfolio in the [operations management workbook](#).

## Guidance to support deliverable completion:

- **Management baseline:**
  - **Inventory and visibility:** Cloud-native tools can help you [collect data](#) and [configure alerts](#). The tools also can help you implement the [monitoring platform](#) that best fits your operating model.
  - **Operational compliance:** The highest percentages of outages tend to come from changes to resource configuration or poor maintenance practices. Follow the [Azure server management guide](#) to implement cloud-native tools to manage patching and changes to resource configuration.
  - **Protection and recovery:** Outages are inevitable on any platform. When a disruption occurs, be prepared with [backup and recovery solutions](#) to minimize the duration.
- **Advanced operations:** Use the management baseline as the foundation for your [business alignment](#) conversations. It helps you to clearly discuss [criticality](#), [business impact](#), and [operations commitments](#). Business alignment helps quantify and validate requests for an [enhanced baseline](#), management of specific [technology platforms](#), or [workload-specific operations](#).
- **Guide an architecture review:** Architecture changes at the workload level might be required to meet operations requirements. The [Microsoft Azure Well-Architected Framework](#) and [Microsoft Azure Well-Architected Review](#) can help guide those conversations with the technical owner of a specific workload.

ACCOUNTABLE TEAM	RESPONSIBLE AND SUPPORTING TEAMS
<ul style="list-style-type: none"><li>● Cloud operations team</li></ul>	<ul style="list-style-type: none"><li>● Cloud strategy team</li><li>● Cloud adoption team</li><li>● Cloud governance team</li><li>● Cloud center of excellence or central IT team</li></ul>

## Step 2: Consistently apply the management baseline

Enterprise reliability requires consistent application of the management baseline. That consistency comes from appropriate corporate policy, IT processes, and automated tools. These resources govern the implementation of the management baseline for all affected resources.

### Deliverables:

- Ensure proper application of the management baseline for all affected systems.
- Document your Resource Consistency policies, processes, and design guidance in the [Resource Consistency discipline template](#).

### Guidance to support deliverable completion:

- Ensure all workloads and resources follow [proper naming and tagging conventions](#). Enforce tagging conventions by using [Azure Policy](#), with a specific emphasis on tags for criticality.
- If you're new to cloud governance, establish [governance policies, processes, and disciplines](#) by using the Govern methodology.
- If you're new to the Cost Management discipline, follow the guidance in the [Cost Management discipline improvements](#) article. Focus on the [implementation](#) section.

### NOTE

**Steps to start reliability partnerships with other teams:** Various decisions throughout the cloud adoption lifecycle can have a direct impact on reliability. The following steps outline the partnerships and supporting efforts required to deliver consistent reliability across the IT portfolio.

ACCOUNTABLE TEAM	RESPONSIBLE AND SUPPORTING TEAMS
<ul style="list-style-type: none"> <li>Cloud governance team</li> </ul>	<ul style="list-style-type: none"> <li>Cloud strategy team</li> <li>Cloud operations team</li> <li>Cloud center of excellence or central IT team</li> </ul>

## Step 3: Define your strategy

Strategic decisions directly affect reliability. They ripple through the adoption lifecycle and into long-term operations. Strategic clarity improves reliability efforts.

### Deliverables:

- Record motivations, outcomes, and business justification in the [strategy and plan template](#).
- Ensure the management baseline provides operational support that aligns to the strategic direction of cloud adoption.

### Guidance to support deliverable completion:

- Understand motivations:** Critical business events and some migration motivations tend to be cost sensitive. These areas can increase the importance of cost control for all later efforts. Other forward-looking motivations related to innovation or growth through migration might be focused more on top-line revenue. Understanding motivations helps you prioritize your cost management.
- Business outcomes:** Some fiscal outcomes tend to be extremely cost sensitive. When the desired outcomes map to fiscal metrics, you should invest early in the Cost Management governance discipline.
- Business justification:** The business justification serves as a high-level view of the overall financial plan for cloud adoption. It can be a good source for initial budgeting efforts.

ACCOUNTABLE TEAM	RESPONSIBLE AND SUPPORTING TEAMS
<ul style="list-style-type: none"> <li>Cloud strategy team</li> </ul>	<ul style="list-style-type: none"> <li>Cloud governance team</li> <li>Cloud operations team</li> <li>Cloud center of excellence or central IT team</li> </ul>

## Step 4: Develop a cloud adoption plan

The digital estate (or analysis of the existing IT portfolio) can help you to validate the business justification. It can provide a refined view of the overall IT portfolio. The adoption plan provides clarity on the timeline of activities during adoption.

When you align the adoption plan with the digital estate analysis, you can plan for future operations management dependencies. Understanding the adoption plan also invites the cloud operations team into the development cycles. They can evaluate and plan for any changes to the management baseline that are required to provide workload operations.

### Deliverables:

- Update the [strategy and plan template](#) to reflect changes that are needed to achieve the desired strategy. The changes recorded can include:
  - An assessment of the existing digital estate.
  - A cloud adoption plan that reflects the required changes and the work involved.

- The organizational change that's required to deliver on the plan.
- A plan for addressing the skills that are needed to enable the existing team to successfully complete the required work.
- Work with the governance team to align cost models and forecast models. This process includes efforts to start optimizing spend through quantitative analysis.

**Guidance to support deliverable completion:**

- [Gather inventory](#): Establish a source of data for analysis of the digital estate prior to adoption.
- [Best practice: Azure Migrate](#): Use Azure Migrate to gather inventory.
- [Incremental rationalization](#): During incremental rationalization, a quantitative analysis can identify cloud candidates for budgeting purposes.
- [Align cost models and forecast models](#): Use Azure Cost Management + Billing to align cost and forecast models by [creating budgets](#).
- [Build your cloud adoption plan](#): Build a plan with actionable workload, assets, and timeline details.

ACCOUNTABLE TEAM	RESPONSIBLE AND SUPPORTING TEAMS
<ul style="list-style-type: none"> <li>Cloud strategy team</li> </ul>	<ul style="list-style-type: none"> <li>Cloud adoption team</li> <li>Cloud governance team</li> <li>Cloud operations team</li> <li>Cloud center of excellence or central IT team</li> </ul>

## Step 5: Implement landing zone best practices

The Ready methodology of the Cloud Adoption Framework focuses heavily on the development of landing zones to host workloads in the cloud. During landing zone implementation, multiple decisions could affect operations. Consult the cloud operations team to help review the landing zone for operations improvements. Also consult the cloud governance team to understand Resource Consistency policies and design guidance that might affect the landing zone design.

**Deliverables:**

- Deploy one or more landing zones capable of hosting workloads in the short-term adoption plan.
- Ensure that all landing zones meet operations decisions and resource consistency requirements.

**Guidance to support deliverable completion:**

- [Improve landing zone operations](#): Best practices for improving operations within a given landing zone.

ACCOUNTABLE TEAM	RESPONSIBLE AND SUPPORTING TEAMS
<ul style="list-style-type: none"> <li>Cloud adoption team</li> </ul>	<ul style="list-style-type: none"> <li>Cloud operations team</li> <li>Cloud strategy team</li> <li>Cloud governance team</li> <li>Cloud center of excellence or central IT team</li> </ul>

## Step 6: Complete waves of adoption effort and change

Long-term operations can be affected by the decisions made during migration and innovation efforts. Maintaining consistent alignment early in adoption processes helps to remove barriers to production releases. It also reduces

the effort that's required to introduce new solutions into operations management practices.

**Deliverables:**

- Test operational readiness of production deployments by using Resource Consistency policies.
- Validate adherence to resource consistency design guidance and operations requirements.
- Document any advanced operations requirements in the [operations management workbook](#).

**Guidance to support deliverable completion:**

- [Environmental readiness checklist](#)
- [Pre-promotion checklist](#)
- [Production release checklist](#)

ACCOUNTABLE TEAM	RESPONSIBLE AND SUPPORTING TEAMS
<ul style="list-style-type: none"><li>• Cloud adoption team</li></ul>	<ul style="list-style-type: none"><li>• Cloud strategy team</li><li>• Cloud operations team</li><li>• Cloud governance team</li><li>• Cloud center of excellence or central IT team</li></ul>

## Value statement

These steps help you to implement the controls and processes that are needed to ensure reliability across the enterprise and all hosted resources.

# Get started: Ensure consistent performance across a portfolio

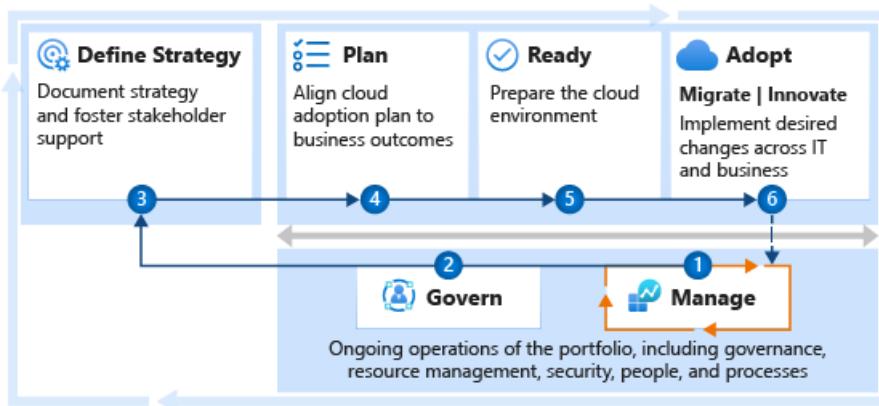
11/9/2020 • 6 minutes to read • [Edit Online](#)

How do you ensure adequate performance across a portfolio of workloads? The steps in this guide can help you establish processes for maintaining that level of performance.

Performance also depends on other roles and functions. This article maps those supporting functions to help you create alignment among the involved teams.

Centralized operations management is the most common approach to consistent performance across the portfolio. Decisions about operational practices define the operations baseline and any holistic enhancements.

The first step in this guide helps the operations team get started. The subsequent steps help the entire enterprise get started on a shared journey toward enterprise performance across the portfolio of workloads.



## Step 1: Establish operations management requirements

The operations management baseline, outlined in the Microsoft Cloud Adoption Framework for Azure, provides a set of controls and cloud-native operations tools to ensure consistent operations. Expanding that baseline with automation tooling provides performance monitoring and automation to meet consistent performance requirements across the portfolio.

### Deliverables:

- Enhance the management baseline to include automated remediation tasks related to deviations from performance expectations.
- When workload-specific data patterns or architecture changes are needed to meet performance requirements, use workload-specific operations to provide greater performance controls.
- Document operational decisions across the IT portfolio in the [operations management workbook](#). Focus on including performance automation decisions in the [Operational Compliance](#) section of the [Baseline](#) tab.

### Guidance to support deliverable completion:

- The [enhanced management baseline](#) article outlines examples of using tools like Azure Automation to add performance-related enhancements. This approach can aid in maintaining consistent performance through basic modifications to the size and scale of supporting assets.
- [Workload-specific operations](#) uses the Microsoft Azure Well-Architected Review to provide guidance on automation for a specific workload. This approach to performance management is particularly useful when

workload-specific data should drive operational actions.

- The preceding guidance assumes that an existing implementation of a [management baseline](#) supports the full portfolio of workloads.

#### NOTE

Various decisions throughout the cloud adoption lifecycle can have a direct impact on performance. The following steps help outline the partnerships and supporting efforts required to deliver performance across the IT portfolio.

ACCOUNTABLE TEAM	RESPONSIBLE AND SUPPORTING TEAMS
<ul style="list-style-type: none"><li>Cloud operations team</li></ul>	<ul style="list-style-type: none"><li>Cloud strategy team</li><li>Cloud adoption team</li><li>Cloud governance team</li><li>Cloud center of excellence or central IT team</li></ul>

## Step 2: Consistent application of the management baseline

As the management baseline is improved, it's important to ensure that those improvements carry through to the Resource Consistency governance discipline. Doing so ensures the application of the enhanced baseline in all managed environments.

#### Deliverables:

- Ensure proper application of the enhanced management baseline for all affected systems.
- Document your policies, processes, and design guidance for resource consistency in the [Resource Consistency discipline template](#).

#### Guidance to support deliverable completion:

- Ensure that all workloads and resources follow [proper naming and tagging conventions](#). Enforce tagging conventions by using [Azure Policy](#), with a specific emphasis on tags for "criticality."
- If you're new to cloud governance, establish [governance policies, processes, and disciplines](#) by using the Govern methodology.
- If you're new to the Cost Management discipline, consider following the [article about Cost Management discipline improvements](#), with a focus on the [implementation](#) section.

ACCOUNTABLE TEAM	RESPONSIBLE AND SUPPORTING TEAMS
<ul style="list-style-type: none"><li>Cloud governance team</li></ul>	<ul style="list-style-type: none"><li>Cloud strategy team</li><li>Cloud operations team</li><li>Cloud center of excellence or central IT team</li></ul>

## Step 3: Define strategy

Strategic decisions directly affect performance, rippling through the adoption lifecycle and into long-term operations. Strategic clarity improves performance efforts across the portfolio. That clarity also helps the operations team understand which workloads need a degree of workload specialization and advanced operations.

#### Deliverables:

- Record motivations, outcomes, and business justification in the [strategy and plan template](#).
- Ensure that the management baseline provides operational support that aligns with the strategic direction of cloud adoption.

#### Guidance to support deliverable completion:

- **Understand motivations:** Critical business events and some migration motivations tend to be cost sensitive, which increases the importance of cost control for all later efforts. Other forward-looking motivations related to innovation or growth through migration might be focused more on top-line revenue. Understanding motivations can help you decide how high to prioritize your cost management.
- **Business outcomes:** Some fiscal outcomes tend to be extremely cost sensitive. When the desired outcomes map to fiscal metrics, you should invest in the Cost Management governance discipline early.
- **Business justification:** The business justification serves as a high-level view of the financial plan for cloud adoption. This can be a good source for initial budgeting efforts.

ACCOUNTABLE TEAM	RESPONSIBLE AND SUPPORTING TEAMS
<ul style="list-style-type: none"> <li>• Cloud strategy team</li> </ul>	<ul style="list-style-type: none"> <li>• Cloud governance team</li> <li>• Cloud operations team</li> <li>• Cloud center of excellence or central IT team</li> </ul>

## Step 4: Assess and plan for workload adoption

The digital estate (or analysis of the existing IT portfolio) can aid in validating the business justification and provide a refined view of the IT portfolio. The adoption plan provides clarity on the timeline of activities during adoption. Aligning that plan and digital estate analysis provides a means of planning for future dependencies on operations management.

Understanding the plan also invites the cloud operations team into the development cycle. The team can then evaluate and plan for any changes to the management baseline that are required to provide workload operations.

#### Deliverables:

- Update the [strategy and plan template](#) to reflect changes triggered by the digital estate analysis.
- Work with the cloud operations team to clearly define the criticality and business impact of each workload in the near-term and long-term adoption plan.
- Work with the cloud operations team to establish a timeline for operations readiness.

#### Guidance to support deliverable completion:

- **Gather inventory:** Establish a source of data for analysis of the digital estate before adoption.
- **Best practice: Azure Migrate:** Use Azure Migrate to gather inventory.
- **Incremental rationalization:** During incremental rationalization, use a quantitative analysis to identify cloud candidates for budgeting purposes.
- **Align cost models and forecast models:** Use Azure Cost Management + Billing to align cost and forecast models by [creating budgets](#).
- **Build your cloud adoption plan:** Build a plan with actionable workload, asset, and timeline details.

ACCOUNTABLE TEAM	RESPONSIBLE AND SUPPORTING TEAMS
------------------	----------------------------------

ACCOUNTABLE TEAM	RESPONSIBLE AND SUPPORTING TEAMS
<ul style="list-style-type: none"> <li>Cloud strategy team</li> </ul>	<ul style="list-style-type: none"> <li>Cloud governance team</li> <li>Cloud operations team</li> <li>Cloud center of excellence or central IT team</li> </ul>

## Step 5: Expand the landing zones

The Ready methodology of the Cloud Adoption Framework focuses heavily on the development of landing zones to host workloads in the cloud. During landing zone implementation, various decisions can affect operations.

Consult the cloud operations team to help review the landing zone for operations improvements. Also consult the cloud governance team to understand "resource consistency" policies and design guidance, which can affect the landing zone design.

### Deliverables:

- Deploy one or more landing zones that can host workloads in the short-term adoption plan.
- Ensure that all landing zones meet operations decisions and resource consistency requirements.

### Guidance to support deliverable completion:

- Improve landing zone operations:** Best practices for improving operations within a landing zone.

ACCOUNTABLE TEAM	RESPONSIBLE AND SUPPORTING TEAMS
<ul style="list-style-type: none"> <li>Cloud adoption team</li> </ul>	<ul style="list-style-type: none"> <li>Cloud operations team</li> <li>Cloud strategy team</li> <li>Cloud governance team</li> <li>Cloud center of excellence or central IT team</li> </ul>

## Step 6: Adoption

Long-term operations might be affected by the decisions that you make during migration and innovation efforts. Maintaining consistent alignment early in adoption processes helps remove barriers to production release. It also reduces the effort required to onboard new solutions into operations management practices.

### Deliverables:

- Test operational readiness of production deployments by using Resource Consistency policies.
- Validate adherence to design guidance for resource consistency and to operations requirements.
- Document any advanced operations requirements in the [operations management workbook](#).

### Guidance to support deliverable completion:

- [Environmental readiness checklist](#)
- [Pre-promotion checklist](#)
- [Production release checklist](#)

ACCOUNTABLE TEAM	RESPONSIBLE AND SUPPORTING TEAMS
------------------	----------------------------------

ACCOUNTABLE TEAM	RESPONSIBLE AND SUPPORTING TEAMS
<ul style="list-style-type: none"><li>• Cloud adoption team</li></ul>	<ul style="list-style-type: none"><li>• Cloud strategy team</li><li>• Cloud operations team</li><li>• Cloud strategy team</li><li>• Cloud governance team</li><li>• Cloud center of excellence or central IT team</li></ul>

## Value statement

The preceding steps will help you implement controls and processes to ensure performance across the enterprise and all hosted resources.

# Get started: Align your organization

11/9/2020 • 3 minutes to read • [Edit Online](#)

Successful cloud adoption is the result of properly skilled people doing the appropriate types of work, in alignment with clearly defined business goals, and in a well-managed environment. To deliver an effective cloud operating model, it's important to establish appropriately staffed organizational structures. This article outlines such an approach.

## Step 1: Understand the functions required for successful cloud teams

The following list outlines the minimum functionality that's required for your organization to succeed at cloud adoption and long-term operations. After you become familiar with the cloud teams and their functions, you can align them with the organizational structure that best fits your staffing and cloud maturity level.

- [Cloud adoption functions](#) deliver technical solutions.
- [Cloud strategy functions](#) align technical change with business needs.
- [Cloud operations functions](#) support and operate adopted solutions.
- [Cloud center of excellence \(CCoE\) functions](#) improve quality, speed, and resiliency of adoption.
- [Cloud governance functions](#) manage risk.
- [Cloud platform functions](#) operate and mature the platform.
- [Cloud automation functions](#) accelerate adoption and innovation.
- [Cloud security functions](#) manage security risks.

## Step 2: Map people to the required functions

The next step is to map specific people to the necessary functions. To do so, answer the following questions:

- What person or group will be responsible for completing technical tasks in the cloud adoption plan?
- What person will be accountable for the team's ability to deliver technical changes?
- What person or group will be responsible for implementing protective governance mechanisms?
- What person will be accountable for defining those governance controls?
- Are there other functions or people that will have accountability or responsibility within the cloud adoption plan?

After you've documented the answers to these questions, see [Plans for skills readiness](#) to help define your plans to prepare these people for forthcoming work.

## Step 3: Determine how teams align within your organization

The following organizational structures don't necessarily have to map to an organizational chart (org chart). Org charts generally reflect command and control management structures. Conversely, the following organizational structures are designed to capture alignment of roles and responsibilities.

In an agile matrix organization, these structures might be best represented as virtual teams. There's nothing to suggest that virtual teams couldn't be represented in an org chart, but a formal org chart isn't necessary to produce an effective operating model.

Determine how the following models fit your organizational structures:

- **Org chart alignment:** Management hierarchies, manager responsibilities, and staff alignment will align with

organizational structures.

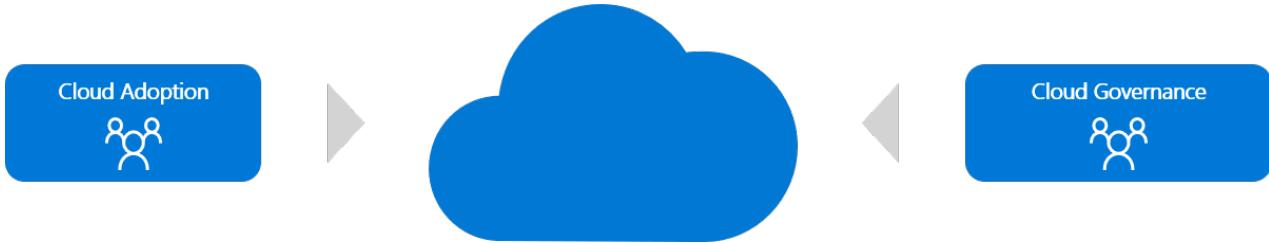
- **Virtual teams:** Management structures and org charts remain unchanged. Instead, virtual teams will be created and tasked with the required functionality.
- **Mixed model:** More commonly, a mixture of org chart and virtual team alignment will be required to deliver on cloud transformation goals.

## Step 4: Establish team structures

During every cloud adoption effort, certain functions must be provided by at least one person. These assignments and team structures can develop organically, or they can be intentionally designed to match a defined team structure.

To help create balance across cloud adoption efforts, we recommend that you start with a minimum of two teams. The following two teams are responsible for various functions throughout the adoption effort:

- **Cloud adoption team:** This team is accountable for technical solutions, business alignment, project management, and operations for the solutions that are adopted.
- **Cloud governance team:** To balance the cloud adoption team, a cloud governance team is dedicated to ensuring excellence in the solutions that are adopted. The cloud governance team is accountable for platform maturity, platform operations, governance, and automation.



This proven approach is considered a minimum viable product (MVP), because it might not be sustainable. Each team wears many hats, as outlined in the [RACI \(responsible, accountable, consulted, and informed\) charts](#).

As adoption needs grow, so does the need to create balance and structure. To meet those needs, companies often follow a process of maturing their organizational structures.

Watch this video to get an overview of common team structures at various stages of organizational maturity.

## Step 5: Align RACI charts

At each level of maturity, accountability for various cloud functions shifts to new teams. This shifting of accountability enables faster migration and innovation cycles by removing and automating barriers to change. To align assignments properly, the [RACI alignment](#) article shows a RACI chart for each organizational structure.

## Additional information

- [Adapt existing roles, skills, and processes for the cloud](#)
- [Organizational antipatterns: Silos and fiefdoms](#)
- [Download the RACI template](#)

# Get started: Build a cloud strategy team

11/9/2020 • 11 minutes to read • [Edit Online](#)

To be successful, every cloud adoption journey needs to involve some level of strategic planning. This getting started guide is designed to help you establish a dedicated team or virtual team that can build and deliver on a solid cloud strategy.

The first step in the journey is to decide whether you need a strategy team, or whether your existing team members can deliver on cloud strategy as a distributed responsibility.

Whichever approach you choose, you'll want to create a cloud strategy team that defines motivations and business outcomes, and that validates and maintains alignment between business priorities and cloud adoption efforts. When the business outcomes affect business functions, the strategy team should include business leaders from across the organization. The goal of the cloud strategy team is to produce tangible business results that are enabled by cloud technologies. Overall, this team ensures that cloud adoption efforts progress in alignment with business outcomes. Whenever possible, business outcomes and the cloud strategy team's efforts should both be defined early in the process.



## NOTE

This article discusses a *strategy facilitator*, a key player in the cloud-adoption process. The role is commonly held by a program manager, architect, or consultant. As the cloud strategy team forms and gets started, the strategy facilitator is temporarily accountable for creating alignment and keeping the team aligned with business goals. The strategy facilitator is often the person most accountable for the success of the cloud adoption journey.

## Step 1: Determine whether a cloud strategy team is needed

A cloud strategy team delivers on a required capability in the cloud, referred to as the cloud strategy capability. Forming a cloud strategy team requires a defined group of dedicated business leaders, stakeholders, and program managers to meet on a regular, recurring basis to advance the strategy that drives cloud adoption.

### Deliverables:

- Determine whether your business requires a cloud strategy team.

### Guidance to support deliverable completion:

Creating a cloud strategy team is often necessary for the following reasons:

REASON	CONSIDERATIONS
Cloud adoption is important to the business.	<ul style="list-style-type: none"> <li>The cloud adoption effort has board-level visibility.</li> <li>Success of the cloud adoption effort will improve market positioning, customer retention, or revenue.</li> <li>The programs in the adoption portfolio map directly to strategic business outcomes.</li> <li>The portfolio of workloads in this adoption effort is strategic and mission-critical and could affect multiple business units.</li> </ul>
Cloud adoption requires ongoing executive support.	<ul style="list-style-type: none"> <li>The cloud adoption effort will affect how you manage organizational change.</li> <li>The effort will require additional training from multiple business users and could interrupt certain business functions.</li> <li>The existing IT operations team or vendor is motivated to remain in an existing datacenter.</li> <li>The existing IT team hasn't fully bought into the effort.</li> </ul>
Cloud adoption presents risk to the business.	<ul style="list-style-type: none"> <li>Failure to complete the migration within the specified time window will result in negative market impact or increased hosting costs.</li> <li>Workloads slated for adoption need to be protected from data leakage that could affect business success or customer security.</li> <li>Metrics that are being used to measure the cloud effort are business aligned, creating a dependency and risk on the technical success.</li> </ul>

If any or all of the preceding reasons represent your existing business considerations, the information in the rest of this article will help you establish your cloud strategy team.

#### Accountable person or team:

- The strategy facilitator is accountable for determining whether a cloud strategy team is needed.

## What if I don't need a cloud strategy team?

Review the [cloud strategy functions](#) that are required to deliver on cloud strategy needs. Not every organization requires a dedicated team or virtual team to help meet its strategic needs. In your [RACI \(responsible, accountable, consulted, and informed\) template](#), list the core accountabilities of the strategy, and identify the person on your team who will be accountable for each. If one person will take on all of those accountabilities, simple replace "cloud strategy" with that person's name in the RACI template.

## Step 2: Establish the cloud strategy team

The cloud strategy team serves as a recurring alignment point between business leaders and IT leaders. Based on the levels of importance, risk, and executive support that drive the need for a strategy team, participation in and the composition of the team might vary.

#### Deliverables:

- Identify the appropriate organizations or individuals who are willing to share in the accountability and responsibility for driving the cloud adoption strategy.

#### Guidance to support deliverable completion:

- Document and share your reasoning from step 1 to identify stakeholders who will benefit from regular involvement and will be able to help drive the strategy.

- For ideas about who might be a good fit, see [Cloud strategy functions](#).
- To validate the alignment and bandwidth from each potential participant, review the [minimum scope](#) and [deliverable](#) for this capability.
- To establish the right RACI chart based on your current team structures, review the various [RACI configuration examples](#), or select one of the example tabs at the bottom of the RACI template.
- Document the results in the [RACI template](#) in the [Org Alignment](#) worksheet.

**Accountable person or team:**

- The strategy facilitator is accountable for establishing the cloud strategy team.

## Step 3: Establish a cadence

Early in the cloud adoption journey, your team will require frequent interaction and iterative strategy reviews. As adoption starts, that frequency will lessen, transitioning to a focus on status and validation or adjustment of the backlog priorities.

Steps 4, 5, and 6 should be completed within four to six weeks. The remaining steps will be completed in subsequent meetings. More frequent meetings should be maintained until the team begins step 7.

**Deliverables:**

Review suggested meeting cadences and schedule meetings with all strategy team participants.

**Guidance to support deliverable completion:**

- Review the suggested short-term and long-term [meeting cadences](#) to align each of the documented participants.

**Accountable person or team:**

- The strategy facilitator is accountable for establishing an appropriate cadence for the cloud strategy team.

## Step 4: Establish a motivation-driven strategy

Cloud adoption journeys include approaches to both migration and innovation. When technical teams define the strategy, it's common for the strategy to be driven by the team members' current skills and strengths. Such a strategy is likely to be a technical success, but it risks producing limited business impact.

The first objective of the cloud strategy team is to define a high-level strategy that's based on business motivations. This can usually be completed in a one-hour workshop with all of the cloud strategy team members. It also requires a minimum of one additional hour to review the business motivations with various technical teams and affected stakeholders.

During the first workshop, each member of the team should prioritize its motivations in the [understand motivations](#) article and share its top priorities. The strategy facilitator helps guide one or more rounds of conversation until a theme emerges in the direction of migration or innovation. There will likely be motivations in the top 3 list from both categories, which might require the team to go deeper on its list before a clear pattern leans one way or another.

This exercise will surface conversations that can help build alignment among the team members. The deliverable will help guide the rest of the strategy and the resulting plan.

**Deliverables:**

- Record motivations in the [strategy and plan template](#).

**Guidance to support deliverable completion:**

- **Understand motivations:** Critical business events and some migration motivations tend to be cost sensitive, which increases the importance of cost control for all subsequent efforts. Other forward-looking motivations that are related to innovation or growth through migration might be focused more on top-line revenue. Understanding motivations helps team members decide how high to prioritize your cost management.

ACCOUNTABLE TEAM	RESPONSIBLE AND SUPPORTING TEAMS
<ul style="list-style-type: none"> <li>• Cloud strategy team</li> </ul>	<ul style="list-style-type: none"> <li>• Cloud governance team</li> <li>• Cloud adoption team</li> <li>• Cloud center of excellence or central IT team</li> </ul>

## Step 5: Establish business outcomes

Each member of the cloud strategy team is asked to define one or more business outcomes by applying specific metrics to measure business success. If a certain metric can be improved as a direct result of the cloud adoption effort, a team member is asked to share the expected impact. If the cloud adoption effort doesn't affect the metric but will enable the business to better drive the metric, that too should be documented.

Many leaders on the cloud strategy team might need to decompose their core metrics to identify an outcome that can be affected or influenced by the cloud adoption effort. If the team members' outcomes can't be affected or influenced by this journey, it might be hard for them to maintain their level of interest in the program. The facilitator should work with each leader to develop an aligned metric and reevaluate whether that team member is the right person to participate on the strategy team.

Impacts on business outcomes can take time. These types of changes typically move slower than technical changes. To maintain transparency, the strategy team should agree on shorter-term learning metrics. These metrics might include technical and other changes that can be reviewed at each team meeting to demonstrate progress toward technical goals and business outcomes.

### Deliverables:

- Identify at least one expected business outcome per member of the cloud strategy team.
- Refine the list of members to align expected time commitments with expected outcomes.
- Align on a set of short-term and mid-term metrics to support ongoing progress reports.

### Guidance to support deliverable completion:

- Record business outcomes in the [strategy and plan template](#).
- **Business outcomes:** Some fiscal outcomes tend to be extremely cost sensitive. When the desired outcomes map to fiscal metrics, it can be wise to invest very early in the Cost Management governance discipline.
- **Learning metrics** help bridge the gap between business outcomes and technical adoption efforts.

### Accountable team:

The cloud strategy team is accountable for defining business outcomes. The team can use specific metrics to measure the success of the business outcomes.

## Step 6: Decide whether to proceed or cancel based on the business justification

Your business justification can help with planning, long-term return expectations, and expectations about total cost of ownership (TCO). In this step, the cloud strategy team should agree on the minimum amount of analysis required to help the strategy team align on a go-forward decision. Strategic alignment might require deep

planning and TCO analysis. Most cloud strategy teams will find a simple cost analysis sufficient to align on direction.

Each member of the strategy team should review common myths and approaches to business justification. This can help the team communicate the specific analysis that's expected from the supporting teams. After the team communicates its expectations, it can reduce its time investment and meeting frequency. The team will maintain accountability for completing the strategy until the business justification and digital estate analysis have been agreed upon.

**Deliverables:**

- Kick off the business justification effort with your supporting teams.
- Meet with the supporting teams monthly (or as needed) until the strategy team can align on a go/no go decision to proceed with cloud adoption.

**Guidance to support deliverable completion:**

- The **business justification** serves as a high-level view of the overall financial plan for cloud adoption. This can be a good source for initial budgeting efforts.

ACCOUNTABLE TEAM	RESPONSIBLE AND SUPPORTING TEAMS
<ul style="list-style-type: none"><li>• Cloud strategy team</li></ul>	<ul style="list-style-type: none"><li>• Cloud governance team</li><li>• Cloud adoption team</li><li>• Cloud center of excellence or central IT team</li></ul>

## Step 7: Support adoption through a regular cadence

After a go-forward decision has been agreed upon with the cloud strategy team, the team can transition into a less intense and less frequent meeting cadence. The expectations of the team also shift at this point. After the journey moves from strategic definition to adoption efforts (plan, ready, adopt), the strategy team is expected to focus on prioritization and strategic support.

**Deliverables:**

- **Prioritization:** When the existing digital estate is rationalized, the strategy team helps establish waves of migration or innovation priorities. This helps the technical implementation teams focus on actions that drive the greatest business value.
- **Evaluate risks:** As cloud adoption grows, new forms of adoption expose new risks. The strategy team is responsible for helping evaluate those new risks. The expectation of the strategy team is to evaluate new risks and determine whether the business can tolerate the risks or it needs policies that eliminate or mitigate them.
- **Review budget and spend:** As cloud adoption increases, so will budgets for various workloads in the portfolio. On a monthly basis, the cloud strategy team should review actual spend against budget to identify issues that need to be resolved. Detecting and addressing budgetary changes early will help prevent sticker shock later in the adoption lifecycle.
- **Business planning:** When the adoption teams complete their migration or innovation efforts, additional business planning will be required to maximize return from the new technology solutions. Such planning might include user training, business process modifications, or other post-adoption activities.
- **Executive support:** Cloud adoption will result in organizational change. This is most visible within the IT organization. At times, various teams or team members might need additional support from the strategy team to understand the changes, develop new skills, and understand how to best operate within the new models.

**Guidance to support deliverable completion:**

- [Incremental rationalization](#): Consider an agile approach to rationalization that properly aligns late-bound technical decisions.
- The [five Rs of rationalization](#): Understand the various rationalization options.

ACCOUNTABLE TEAM	RESPONSIBLE AND SUPPORTING TEAMS
<ul style="list-style-type: none"> <li>• Cloud strategy team</li> </ul>	<ul style="list-style-type: none"> <li>• Cloud governance team</li> <li>• Cloud adoption team</li> <li>• Cloud center of excellence or central IT team</li> </ul>

## What's next

Strategy and planning are important. Nothing is actionable until you identify the cloud adoption functions that are needed on your team. It's important to understand these key capabilities before you begin your adoption efforts.

Align your strategy with the [cloud adoption functions](#) by working with the adoption team or individuals who are responsible for these functions.

Learn to align responsibilities across teams by developing a cross-team matrix that identifies RACI parties.

Download and modify the [RACI template](#).

# Get started: Build a cloud adoption team

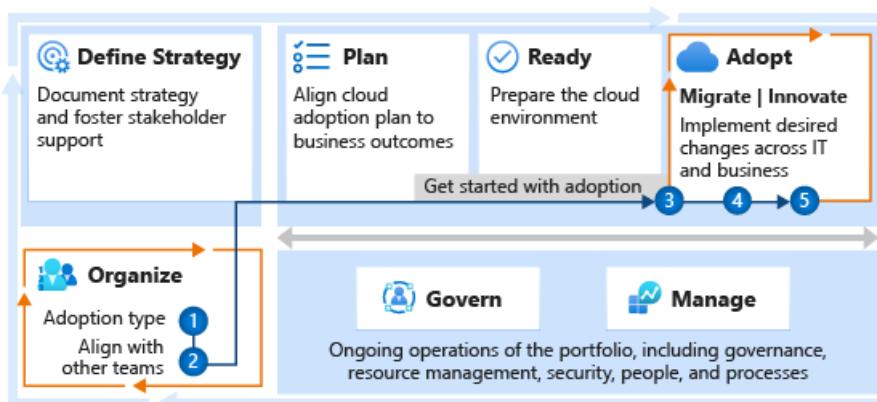
11/9/2020 • 6 minutes to read • [Edit Online](#)

Cloud adoption teams are the modern-day equivalent of technical implementation teams or project teams. The nature of the cloud might require more fluid team structures.

Some cloud adoption teams focus exclusively on cloud migration, and others focus on innovations that take advantage of cloud technologies. Some teams include the broad technical expertise that's required to complete large adoption efforts, such as a full datacenter migration, and others have a tighter technical focus.

A smaller team might move between projects to accomplish specific goals. For example, a team of data platform specialists might focus on helping convert SQL Database virtual machines (VMs) to SQL PaaS instances.

As cloud adoption expands, customers benefit from a team that's dedicated to the [cloud platform function](#). That team uses automated deployment and code reuse to accelerate successful adoption. People focused on a cloud platform function can implement infrastructure, application patterns, governance, and other supporting assets to drive further efficiencies and consistency, and to instill cloud principles in your organization. Small organizations and small adoption teams don't have the luxury of a dedicated cloud platform team. We recommend that you establish an automation capability in your adoption team to begin building this important cloud muscle.



## Step 1: Determine the type of adoption team you need

Cloud adoption teams tend to perform one or more of the following types of adoption:

- Migration of existing workloads
- Modernization of existing workloads and assets
- Architectural change to existing workloads and assets
- Development of new workloads

The adoption of any IT portfolio will likely require a mixture of these types of efforts. Unfortunately, each type requires different skills and mindsets. The more specialized an adoption team, the more effective and efficient the team will be when it delivers that type of work. Conversely, mastery of all the implementation options across cloud adoption can be overwhelming for these more specialized teams.

When you're first building a cloud adoption team, aligning with one of the Adopt methodologies will help accelerate the development of the team's collective skills.

### Deliverables:

- Determine whether the team aligns better with the Migrate methodology or the Innovate methodology.
- Each methodology has a four-step onboarding experience to help the team understand the tools and processes

required to get really good at that effort. Invest time as a team going through the first few steps to understand which tools and scenarios you're most likely to need in early iterations.

- Align responsibilities across teams by developing a cross-team matrix that identifies *responsible, accountable, consulted, and informed (RACI)* parties. Update your company's [RACI template](#) to help others understand who's on the team and which methodology the team will focus on delivering.

#### Guidance to support deliverable completion:

- [Migrate methodology overview](#) describes the process, tools, and approaches for migrating and modernizing a portfolio of workloads.
- [Innovate methodology overview](#) describes the process, tools, and approaches for adding cloud-native workloads to the portfolio.
- [Understand motivations](#) behind this effort to see whether they're better aligned with migration or innovation efforts.

## Step 2: Align your team with other supporting teams

If your company's cloud adoption effort is mature enough to have supporting teams, you might be able to find a list of the teams and subject matter experts in your company's version of the [RACI template](#), including cloud governance, cloud operations, a cloud center of excellence, or other similar teams.

#### Deliverables:

- Review design guidance, operational baselines, policies, and processes from the various supporting teams to understand the guardrails that have been established for guiding cloud adoption.
- Review the guidance with other cloud adoption teams to understand any limitations you might encounter as a result of those guardrails.

#### Guidance to support deliverable completion:

- [Evaluate corporate policy](#) outlines the steps to define corporate policy, which might limit decisions that the team can safely make in the company's cloud environment.
- [Governance disciplines](#) outlines the types of controls or disciplined processes that the governance team has likely implemented to allow for safe, compliant adoption of the cloud.
- The [Manage methodology](#) outlines the considerations that go into a cloud operations baseline for providing basic operations management.

ACCOUNTABLE TEAM	RESPONSIBLE AND SUPPORTING TEAMS
<ul style="list-style-type: none"><li>● The cloud strategy team is accountable for maintaining a clear RACI structure across the cloud adoption lifecycle.</li></ul>	<p>Review guidance and requirements from:</p> <ul style="list-style-type: none"><li>● Cloud governance team</li><li>● Cloud operations team</li><li>● Cloud center of excellence or central IT team</li><li>● Other cloud adoption teams or individuals listed in the RACI</li></ul>

## Step 3: Begin your adoption journey

Depending on the type of adoption team you're a member of, you'll get started with one of these guides:

- [Get started: Migrate workloads to the cloud](#)
- [Get started: Build new products or services](#)

These guides provide guidance for various teams listed alongside their varying degrees of accountability and

responsibility. Use the guides to understand how your team fits into the rest of the journey. Also use them to understand the levels of support you can expect to get from around the company.

In the end, the cloud adoption team is accountable for delivery across their assigned migration efforts or new product development. Although supporting teams are accountable for ensuring that each step is completed, it's the responsibility of each cloud adoption team to ensure that the supporting team is getting the support it needs to be successful. If the accountable team doesn't yet exist or needs more support to deliver on its accountable steps, the adoption team is encouraged to partner with other teams to complete its deliverables.

**Deliverables:**

- Become increasingly better at delivering on the methodology associated with your adoption approach.
- Support other teams in the completion of their accountable steps, even if those steps are blockers to your adoption efforts.

**Guidance to support deliverable completion:**

- In the getting started guide for migration, the adoption team is accountable for delivery of [step 10: Migrate your first workload](#).
- In the getting started guide for new products, the adoption team is accountable for delivery of [step 8: Innovate in the cloud](#).

All other steps on those checklists are designed to make the effort more manageable.

ACCOUNTABLE TEAM	RESPONSIBLE AND SUPPORTING TEAMS
<ul style="list-style-type: none"><li>• Cloud adoption team</li></ul>	<ul style="list-style-type: none"><li>• Cloud governance team</li><li>• Cloud operations team</li><li>• Cloud center of excellence or central IT team</li><li>• Cloud strategy team</li></ul>

## Step 4: Expand your skills with scenarios and best practices

After one or two iterations, the cloud adoption team will understand the basics of their primary methodology. From there, the team will likely be ready to take on additional scenarios and start implementing some additional best practices.

**Deliverables:**

- Increase skills and experience to address more complex adoption scenarios.

**Guidance to support deliverable completion:**

The team can review and expand their skills by reviewing the following guidance:

- Migrate new types of workloads or solve more complex migration challenges through [scenarios](#) and [best practices](#).
- Innovate by using new cloud-native solutions, or solve more complex innovation challenges through [scenarios](#) and [best practices](#).

**Accountable team:**

- The cloud adoption team is accountable for expanding its skills.

## Step 5: Build a cloud adoption factory

As the team becomes more familiar with various adoption scenarios, it will be able to do more and do it faster. This section of guidance will take the team's adoption abilities to the next level.

The cloud adoption factory approach looks at the processes behind adoption efforts. Because of a lack of understanding and clear communication, most of the time burden that's related to migration and innovation comes from a high volume of meetings. Clearly defining processes and interactions at various phases of the cloud adoption journey will remove cultural and political blockers.

**Deliverables:**

- Improve delivery processes to create a highly optimized adoption factory.

**Guidance to support deliverable completion:**

- Process guidance that supports [migration efforts](#) can be found in the process improvements section of the Migrate methodology.
- In the Innovate methodology, the guidance focuses on [innovation processes](#) that result in less technology and more effective product development.

**Accountable team:**

- The cloud adoption team is accountable for building the processes that take adoption to the next level.

## What's next

Cloud adoption is a great goal, but ungoverned adoption can produce unexpected results. To accelerate adoption and best practices, as you're reducing business and technical risks, align cloud adoption with [cloud governance functions](#).

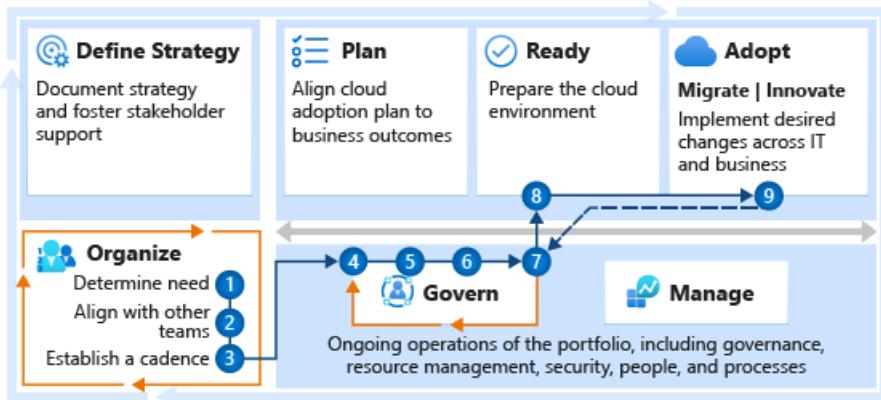
Aligning with the cloud governance team creates balance across cloud adoption efforts, but this is considered a minimum viable product (MVP), because it might not be sustainable. Each team is wearing many hats, as outlined in the [RACI charts](#).

Learn more about overcoming [organizational antipatterns: silos and fiefdoms](#).

# Get started: Build a cloud governance team

11/9/2020 • 6 minutes to read • [Edit Online](#)

A cloud governance team ensures that cloud-adoption risks and risk tolerance are properly evaluated and managed. The team identifies risks that can't be tolerated by the business, and it converts risks into governing corporate policies.



## Step 1: Determine whether a cloud governance team is needed

The official guidance in the Cloud Adoption Framework is to always create a cloud governance team. At first, the team might be very small. Regardless of its size, its role is important. If a team isn't needed, a group or individual on an existing adoption team should agree to fulfill the responsibilities associated with [cloud governance functions](#).

### Deliverables:

- Determine whether you need a cloud governance team.
- Align responsibilities across teams by developing a cross-team matrix that identifies *responsible, accountable, consulted, and informed (RACI)* parties. Document the decision and the responsible individuals using the [RACI template](#) in the [Org Alignment](#) worksheet.

### Guidance to support deliverable completion:

- [Cloud governance functions](#) might already be spread across multiple individuals or teams. Having a team that goes by the title "cloud governance team" isn't important, but the required capabilities should reside with an accountable party or team.
- If the company's long-term cloud adoption strategy can be delivered from one landing zone in one cloud environment, the amount of governance and operations efforts might be small enough for delivery by one person or one team. That team is unlikely to be called cloud governance, because it serves many functions beyond cloud governance. Even for that team, this getting started guide can help ensure that it can deliver on this important function of governance.

ACCOUNTABLE TEAM	RESPONSIBLE AND SUPPORTING TEAMS
<ul style="list-style-type: none"><li>• Cloud strategy team</li></ul>	<ul style="list-style-type: none"><li>• Cloud adoption team</li></ul>

## Step 2: Align with other teams

The governance team ensures consistency and adherence to a set of common policies. Those policies come from an ongoing alignment with other teams.

Before it establishes policies or automated cloud governance, the cloud governance team should meet with other teams that are identified in the RACI template. This will help ensure alignment on critical topics, such as security, cost, performance, operations, and deployment. Steps 4 and 5 can help facilitate the alignment.

**Deliverables:**

- Discuss current-state implementation and ongoing adoption plans with each team.

**Guidance to support deliverable completion:**

- Review your company's [strategy and plan template](#) with members of the cloud strategy team to understand motivations, metrics, and strategy.
- Review your company's [cloud adoption plan](#) with members of the cloud adoption team to understand timelines and prioritization.
- Review the operation team's [operations management workbook](#) to understand the operational requirements and commitments that have been established with the business.

ACCOUNTABLE TEAM	RESPONSIBLE AND SUPPORTING TEAMS
<ul style="list-style-type: none"><li>• Cloud governance team</li></ul>	<ul style="list-style-type: none"><li>• Cloud strategy team</li><li>• Cloud adoption team</li><li>• Cloud operations team</li><li>• Cloud center of excellence or central IT team</li></ul>

## Step 3: Establish a cadence with other teams

Cloud adoption generally comes in waves, or releases. A regular cadence that's aligned with those releases lets the cloud governance team look ahead and understand the risks that will be introduced in the next wave. Staying engaged with the strategy, adoption, and operations teams during planning and review also helps the governance team stay ahead of coming risks.

**Deliverables:**

- Establish a cadence with the supporting teams. If possible, align that cadence with release and planning cycles.
- Establish a separate cadence directly with the cloud strategy team (or various team members) to review risks that are associated with the next wave of adoption and gauge the team's level of tolerance for those risks.

**Guidance to support deliverable completion:**

- For more guidance on cadences for meetings, see [Cloud governance functions](#).

ACCOUNTABLE TEAM	RESPONSIBLE AND SUPPORTING TEAMS
<ul style="list-style-type: none"><li>• Cloud governance team</li></ul>	<ul style="list-style-type: none"><li>• Cloud strategy team</li><li>• Cloud adoption team</li><li>• Cloud operations team</li></ul>

## Step 4: Review the methodology

To help establish a future vision for governance and a working approach to that vision, review the Govern

methodology of the Cloud Adoption Framework.

**Deliverables:**

- Gain an understanding of the methodology, approach, and implementation that supports the Govern methodology.

**Guidance to support deliverable completion:**

- Review the [Govern methodology](#).

**Accountable team:**

- The cloud governance team is accountable for establishing a vision and approach to governance.

## Step 5: Complete the governance benchmark

Governance is a broad topic. A short assessment can help the team understand where to get started.

**Deliverables:**

- Complete the governance benchmark assessment, based on conversations with various stakeholders. Or ask other teams to complete the assessment on their own.

**Guidance to support deliverable completion:**

- Use the [governance benchmark](#) to assess your governance needs and priorities.

**Accountable team:**

- The cloud governance team should understand the gaps that are identified in the governance benchmark and then provide direction on governance that helps address the gaps.

## Step 6: Implement the initial governance best practice and configuration

The Govern methodology includes two approaches to an initial governance foundation. Review each approach, and implement the one that most closely matches your needs.

**Deliverables:**

- Deploy the basic governance tools and organization configurations that are required to govern the environment during the next few waves of adoption efforts.

**Guidance to support deliverable completion:**

- For guidance on configuration and implementation, review [establish an initial cloud governance foundation](#).

**Accountable team:**

- The cloud governance team is accountable for the review and implementation of governance best practices and an initial governance foundation.

## Step 7: Continuously improve governance maturity

Governance needs grow as additional cloud adoption efforts are completed. Stay aligned with the ongoing adoption plan to ensure that the governance approach can maintain the proper levels of governance and control.

**Deliverables:**

- Implement governance improvements to guard against changing risks and governance needs.

#### **Guidance to support deliverable completion:**

- To help improve the initial governance foundation, implement [expanded governance scenarios](#).

#### **Accountable team:**

- The cloud governance team is accountable for aligning with ongoing adoption plans.

## **Step 8: Evaluate landing zone changes**

As landing zones are deployed and expanded, new risks or governance violations might emerge. Periodically review landing zone configurations to identify any deviations from policy that aren't caught by the cloud-native governance tools. Ensure that each landing zone deployment adheres to guidelines for landing zone governance.

#### **Deliverables:**

- Help the cloud platform team develop improvements to the landing zone, which must comply with governance policies.

#### **Guidance to support deliverable completion:**

- Improve [landing zone governance](#).

#### **Accountable team:**

- The cloud governance team should make sure that each landing zone deployment adheres to governance guidelines.

## **Step 9: Adoption handoffs**

As new adoption efforts are completed, the cloud adoption team hands off operational responsibilities to the cloud operations team and cloud governance teams. Stay aligned with adoption release cadences to ensure proper documentation and policy alignment, and to help the team assume responsibility for the workloads.

#### **Deliverables:**

- Regularly review and accept handoffs from other cloud adoption teams.

#### **Guidance to support deliverable completion:**

- Establish a process for [onboarding new workloads and resources](#).

ACCOUNTABLE TEAM	RESPONSIBLE AND SUPPORTING TEAMS
<ul style="list-style-type: none"><li>• Cloud adoption teams</li></ul>	<ul style="list-style-type: none"><li>• Cloud governance team</li><li>• Cloud operations team</li></ul>

## **What's next**

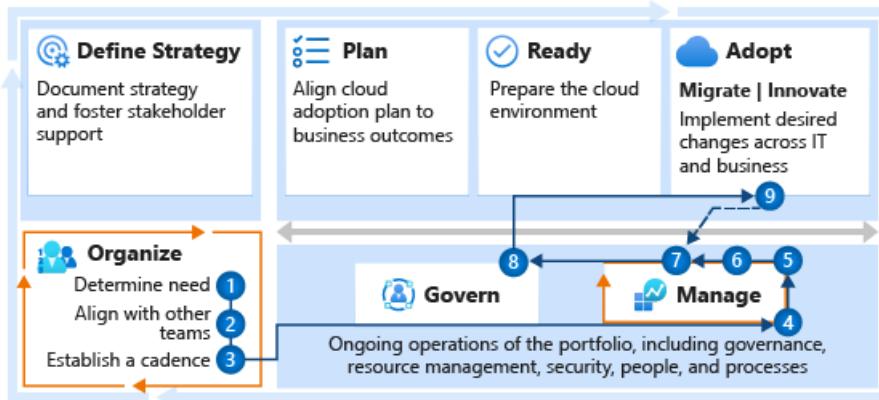
All companies are unique, and so are their governance needs. Choose the level of maturity that fits your organization, and use the Cloud Adoption Framework to guide the practices, processes, and tooling that can help you get there.

As cloud governance matures, teams are empowered to adopt the cloud at a faster pace. Continuous cloud adoption efforts tend to trigger maturity in IT operations. To ensure that governance is a part of operations development, either develop a [cloud operations team](#) or sync with your existing cloud operations team.

# Get started: Build a cloud operations team

11/9/2020 • 6 minutes to read • [Edit Online](#)

An operations team focuses on monitoring, repairing, and remediating issues related to traditional IT operations and assets. In the cloud, many of the capital costs and operations activities are transferred to the cloud provider, giving IT operations the opportunity to improve and provide significant additional value.



## Step 1: Determine whether a cloud operations team is needed

Before you can release any workloads into production, an agreement must be reached on the accountability for delivery of [cloud operations functions](#). For some portfolios, operational responsibilities might belong to the DevOps and cloud adoption teams. In other cases, a managed service provider with cloud operations experience might assume ongoing operational duties.

If no DevOps or service-provider operations agreements are in place, it's safe to assume that someone within IT will need to commit to ongoing operational duties regarding the management of production workloads.

### Deliverables:

- Determine whether you need a cloud operations team.
- Align responsibilities across teams by developing a cross-team matrix that identifies *responsible, accountable, consulted, and informed (RACI)* parties. Document the decision and responsible individuals in the [RACI template](#) in the [Org Alignment](#) worksheet.

### Guidance to support deliverable completion:

- [Cloud operations functions](#) might be spread across multiple individuals or teams already. Decide whether a cloud operations team is required. Some level of operations is always needed for production workloads.
- If the company's long-term cloud adoption strategy can be delivered from one landing zone in one cloud environment, the governance and operations efforts might be small enough to be delivered by one person or one team. That team is unlikely to be called cloud operations, because it will serve many functions. For that individual or team, the following guidance can help ensure that it can deliver on this important function of operations.

ACCOUNTABLE TEAM	RESPONSIBLE AND SUPPORTING TEAMS
<ul style="list-style-type: none"><li>• Cloud strategy team</li></ul>	<ul style="list-style-type: none"><li>• Cloud adoption team</li><li>• Cloud governance team</li></ul>

## Step 2: Align with other teams

The cloud operations team inherits operational responsibilities for all workloads in the production portfolio. Those responsibilities can vary between workloads, based on expectations and the commitments the team has made to business stakeholders. The architectural decisions made by migration-focused and innovation-focused cloud adoption teams also influence the team's operational commitments.

Before the cloud operations team implements any ongoing operations practices, it's important for it to align with other teams. The team should meet with other teams that are identified in the RACI template to ensure alignment on critical topics, such as security, cost, performance, governance, adoption, and deployment. Steps 4 and 5 can help facilitate this alignment.

### Deliverables:

- Discuss current-state implementation and ongoing adoption plans with each team.

### Guidance to support deliverable completion:

- To understand team motivations, metrics, and strategy, review your company's [strategy and plan template](#) with members of the cloud strategy team.
- To understand timelines and prioritization, review your company's [cloud adoption plan](#) with members of the cloud adoption team.
- To understand the operational requirements and commitments that the team has established with the business, begin developing the [operations management workbook](#).

ACCOUNTABLE TEAM	RESPONSIBLE AND SUPPORTING TEAMS
<ul style="list-style-type: none"><li>• Cloud operations team</li></ul>	<ul style="list-style-type: none"><li>• Cloud strategy team</li><li>• Cloud adoption team</li><li>• Cloud governance team</li><li>• Cloud center of excellence or central IT team</li></ul>

## Step 3: Establish a cadence with other teams

Cloud adoption generally comes in waves, or releases. A regular cadence that's aligned with those releases lets the cloud operations team prepare for the handoffs at the end of the next wave. Staying engaged with the strategy, adoption, and governance teams during planning and review helps the operations team stay ahead of the coming operational demands.

### Deliverables:

- Establish a cadence with the supporting teams. If possible, align that cadence with release and planning cycles.
- Establish a separate cadence directly with the cloud strategy team or its various team members to review any operational requirements that are associated with the next wave of adoption.

### Guidance to support deliverable completion:

- For additional guidance on cadences for meetings, see the "deliverables" section of [cloud operations functions](#).

ACCOUNTABLE TEAM	RESPONSIBLE AND SUPPORTING TEAMS
------------------	----------------------------------

ACCOUNTABLE TEAM	RESPONSIBLE AND SUPPORTING TEAMS
<ul style="list-style-type: none"> <li>Cloud operations team</li> </ul>	<ul style="list-style-type: none"> <li>Cloud strategy team</li> <li>Cloud adoption team</li> <li>Cloud governance team</li> </ul>

## Step 4: Review the methodology

To help establish a future vision for operations management and a working approach to achieve that vision, review the Manage methodology of the Cloud Adoption Framework.

### Deliverables:

- Gain an understanding of the methodology, approach, and implementation that supports the Manage methodology.

### Guidance to support deliverable completion:

- Review the [Manage methodology of the Cloud Adoption Framework](#).

### Accountable team:

- The cloud operations team is accountable for the vision and approach to operations management.

## Step 5: Implement the operations baseline

If operations practices aren't already deployed to your cloud environments, start with the operations baseline. That baseline will implement cloud-native, no-ops/low-ops practices to provide a base level of operational protection.

### Deliverables:

- Deploy the basic Azure server-management configurations that are required for operating the environment during the next few waves of adoption efforts.

### Guidance to support deliverable completion:

- Implement the [operations baseline configuration](#).

### Accountable team:

- The cloud operations team is accountable for implementing the operations baseline.

## Step 6: Align business commitments

Review the team's operations baseline commitments with the business stakeholders. This baseline helps you evaluate the general requirements for the majority of workloads. The process also helps you identify the stakeholders for various workloads and enables you to document their ongoing operational expectations.

### Deliverables:

- Document the expectations of business stakeholders.
- Determine whether advanced operations are required for specific workloads or platforms.

### Guidance to support deliverable completion:

- Create [business alignment](#) in the cloud.
- Document the portfolio and operations expectations in the [operations management workbook](#).

### Accountable team:

- The cloud operations team should understand the business expectations, and it's accountable for ongoing alignment with those expectations.

## Step 7: Operations maturity

By continually making operational improvements, the team can:

- Enhance the operations baseline.
- Improve platform operations.
- Implement workload-specific operations.

As additional workloads are transitioned to cloud operations, the need for operations improvements become clearer.

**Deliverables:**

- Improve operations maturity to support commitments to business stakeholders.

**Guidance to support deliverable completion:**

- Evaluate the best options for [advanced operations management](#).

**Accountable team:**

- The cloud operations team is accountable for operational improvements and maturity over time.

## Step 8: Scale operations consistency through governance

As operations planning continues to mature, the team should coordinate with the cloud governance team regularly to apply operations requirements across the portfolio.

**Deliverables:**

- Help the cloud governance team implement new requirements for resource consistency.

**Guidance to support deliverable completion:**

- Review the [governance guide for improving resource consistency](#).

ACCOUNTABLE TEAM	RESPONSIBLE AND SUPPORTING TEAMS
• Cloud governance team	• Cloud operations team

## Step 9: Adoption handoffs

As new adoption efforts are completed, the cloud adoption team hands off operational responsibilities to the cloud operations and cloud governance teams. To ensure proper documentation and policy alignment, and to assume responsibility for the workloads, the team should stay aligned with adoption releases.

**Deliverables:**

- Regularly review and accept handoffs from cloud adoption teams.

**Guidance to support deliverable completion:**

- Establish a process for [onboarding new workloads and resources](#).

ACCOUNTABLE TEAM	RESPONSIBLE AND SUPPORTING TEAMS
<ul style="list-style-type: none"><li>• Cloud adoption teams</li></ul>	<ul style="list-style-type: none"><li>• Cloud governance team</li><li>• Cloud operations team</li></ul>

## What's next

As adoption and operations scale, it's important to define and automate governance best practices that extend existing IT requirements. Forming a cloud center of excellence (CCoE) team is an important step toward scaling cloud adoption, cloud operations, and cloud governance efforts.

Learn more about:

- [Cloud center of excellence functions](#)
- [Organizational antipatterns: Silos and fiefdoms](#)

Align responsibilities across teams by developing a cross-team matrix that identifies RACI parties. Download and modify the [RACI template](#).

# Develop a cloud adoption strategy

11/9/2020 • 2 minutes to read • [Edit Online](#)

The cloud delivers fundamental technology benefits that can help your enterprise execute multiple business strategies. By using cloud-based approaches, you can improve business agility, reduce costs, accelerate time to market, and enable expansion into new markets. To take advantage of this great potential, start by documenting your business strategy in a way that's both understandable to cloud technicians and palatable to your business stakeholders.

The following steps can help you document your business strategy efficiently. This approach helps you drive adoption efforts that capture targeted business value in a cross-functional model. Then, you can map your cloud adoption strategy to specific cloud capabilities and business strategies to reach your desired state of transformation.

1	<p><a href="#">Define and document your motivations:</a> Meet with key stakeholders and executives to document the motivations behind cloud adoption.</p>
2	<p><a href="#">Document business outcomes:</a> Engage motivated stakeholders and executives to document specific business outcomes.</p>
3	<p><a href="#">Develop a business case:</a> Develop a business case to validate the financial model that supports your motivations and outcomes.</p>
4	<p><a href="#">Choose the right first project:</a> Your first cloud adoption project will help align motivations with technical effort. This article can help you choose your first project wisely.</p>

Use the [strategy and plan template](#) to build out your cloud adoption strategy, and to track the output of each of the steps outlined above.

# Motivations: Why are we moving to the cloud?

11/9/2020 • 4 minutes to read • [Edit Online](#)

"Why are we moving to the cloud?" It's a common question for business and technical stakeholders alike. If the answer is, "Our board (or CIO, or C-level executives) told us to move to the cloud," then it's unlikely that the business will achieve the desired outcomes.

This article discusses a few motivations behind cloud migration that can help produce more successful business outcomes. These options help facilitate a conversation about motivations and, ultimately, business outcomes.

## Motivations

Business transformations that are supported by cloud adoption can be driven by various motivations. It's likely that several motivations apply at the same time. The goal of the lists in the following table is to help generate ideas about which motivations are relevant. From there, you can prioritize and assess the potential impacts of the motivations. In this article, your cloud adoption team should meet with various executives and business leaders using the list below to understand which of these motivations are affected by the cloud adoption effort.

CRITICAL BUSINESS EVENTS	MIGRATION	INNOVATION
Datacenter exit	Cost savings	Preparation for new technical capabilities
Merger, acquisition, or divestiture	Reduction in vendor or technical complexity	Building new technical capabilities
Reduction in capital expenses	Optimization of internal operations	Scaling to meet market demands
End of support for mission-critical technologies	Increase in business agility	Scaling to meet geographic demands
Response to regulatory compliance changes	Preparation for new technical capabilities	Improved customer experiences and engagements
New data sovereignty requirements	Scaling to meet market demands	Transformation of products or services
Reduction of disruptions and improvement of IT stability	Scaling to meet geographic demands	Market disruption with new products or services
Reduce carbon footprint	Integration of a complex it portfolio	Democratization and/or self-service environments

## Classify your motivations

Your motivations for cloud adoption will likely fall into multiple categories. As you're building the list of motivations, trends will likely emerge. Motivations tend to be associated more with one classification than with others. Use the predominant classification to help guide the development of your cloud adoption strategy.

When a response to critical business events is the highest priority, it's important to [get started with migration](#) early, often in parallel with strategy and planning efforts. Taking this approach requires a growth mindset and a willingness to iteratively improve processes, based on direct lessons learned.

When migration is the highest priority, strategy and planning will play a vital role early in the process. We recommend that you implement the first workload in parallel with planning efforts, to help the team

understand and anticipate any learning curves that are associated with cloud adoption.

When innovation is the highest priority, strategy and planning require additional investments early in the process to ensure balance in the portfolio and wise alignment of the investment made during cloud adoption. For further information and guidance, see [Understand the innovation journey](#).

To ensure wiser decision-making, all participants in the migration process should have a clear awareness of their motivations. The following section outlines how customers can guide and effect wiser decisions through consistent, strategic methodologies.

## Motivation-driven strategies

This section highlights the *migration* and *innovation* motivations and their corresponding strategies.

### Migration

The *migration* motivations listed near the top of the motivations table are the most common, but not necessarily the most significant, reasons for adopting the cloud. These outcomes are important to achieve, but they're most effectively used to transition to other, more useful worldviews. This important first step to cloud adoption is often called a *cloud migration*. The framework refers to the strategy for executing a cloud migration by using the term [migrate](#).

Some motivations align well with a migrate strategy. The motives at the top of this list will likely have significantly less business impact than those toward the bottom of the list.

- Cost savings.
- Reduction in vendor or technical complexity.
- Optimization of internal operations.
- Increasing business agility.
- Preparing for new technical capabilities.
- Scaling to meet market demands.
- Scaling to meet geographic demands.

### Innovation

Data is the new commodity. Modern applications are the supply chain that drives that data into various experiences. In today's business market, it's hard to find a transformative product or service that isn't built on top of data, insights, and customer experiences. The motivations that appear lower in the *innovation* list align to a technology strategy referred to in this framework as the [Innovate methodology](#).

The following list includes motivations that cause an IT organization to focus more on an innovate strategy than a migrate strategy.

- Increasing business agility.
- Preparing for new technical capabilities.
- Building new technical capabilities.
- Scaling to meet market demands.
- Scaling to meet geographic demands.
- Improving customer experiences and engagements.
- Transforming products or services.

## Next steps

Understanding projected business outcomes helps facilitate the conversations that you need to have as you document your motivations and supporting metrics, in alignment with your business strategy. Next, read an overview of business outcomes that are commonly associated with a move to the cloud.

## Overview of business outcomes

# What business outcomes are associated with transformation journeys?

11/9/2020 • 2 minutes to read • [Edit Online](#)

The most successful transformation journeys start with a business outcome in mind. Cloud adoption can be a costly and time-consuming effort. Fostering the right level of support from IT and other areas of the business is crucial to success. This article series is designed to help customers identify business outcomes that are concise, defined, and drive observable results or change in business performance, supported by a specific measure.

During any cloud transformation, the ability to speak in terms of business outcomes supports transparency and cross-functional partnerships. The business outcome framework starts with a simple template to help technically minded individuals document and gain consensus. This template can be used with several business stakeholders to collect a variety of business outcomes, which could each be influenced by a company's transformation journey. Feel free to use this template electronically or, better still, draw it on a whiteboard to engage business leaders and stakeholders in outcome-focused discussions.

To learn more about business outcomes and the business outcome template, see [Documenting business outcomes](#), or download the [business outcome template](#).

## Prepare for conversations with different personas

The following are a few business outcomes that tend to trigger conversations with various personas:

- **Finance leadership:** Increase profitability while driving compliance.
- **Marketing:** Acquire and retain customers, build reputation.
- **Sales:** Accelerate sales, improve customer lifetime value.
- **Human resources:** Retain, recruit, and empower employees.
- **Executive leadership:** Meeting market growth requirements and environmental sustainability metrics.

## Sample outcomes by category

Speaking in business outcomes can feel like a foreign language to many technically minded individuals. To help ease translation, we curate a set of business outcome examples. You can use the following examples to inspire and demonstrate business outcomes that are based on actual transformation journeys.

To help you find business outcomes more easily, we've separated them into the following categories. This approach tends to drive consensus-building conversations across business units.

### Fiscal outcomes

Financial or fiscal performance is the cleanest business outcome for many business leaders, but not the only one.

[View samples of fiscal outcomes.](#)

### Agility outcomes

Today's fast-changing business environment places a premium on time. The ability to respond to and drive market change quickly is the fundamental measure of business agility.

[View samples of agility outcomes.](#)

## **Reach outcomes**

In a constantly shrinking market, global reach (ability to support global customers and users) can be measured by compliance in geographies that are relevant to the business.

View outcomes related to [global reach](#).

## **Customer engagement outcomes**

Social marketplaces are redefining winners and losers at an unheard-of pace. Responding to user needs is a key measure of customer engagement.

Learn more about [customer engagement outcomes](#).

## **Performance outcomes**

Performance and reliability are assumed. When either falters, reputation damage can be painful and long-lasting.

Learn more about [performance outcomes](#).

## **Sustainability goals**

Organizations are increasingly discussing environmental goals and sustainability targets.

Learn more about [sustainability goals](#).

Each of the business outcomes listed in the preceding categories can help facilitate a focused conversation among your business and technical team members. However, you shouldn't limit your conversations to these generic samples. Understanding the unique needs of your own business, and building outcomes that match, maximizes the value of a cloud transformation.

## **Next steps**

Learn more about [fiscal outcomes](#).

[Fiscal outcomes](#)

# Data innovations

11/9/2020 • 4 minutes to read • [Edit Online](#)

Many companies want to migrate their existing data warehouse to the cloud. They are motivated by a number of factors, including:

- No hardware to buy or maintenance costs.
- No infrastructure to manage.
- The ability to switch to a secure, scalable, and low-cost cloud solution.

For example, the cloud-native, pay-as-you-go service from Azure called Azure Synapse Analytics provides an analytical database management system for organizations. Azure technologies help modernize your data warehouse after it's migrated and extend your analytical capabilities to drive new business value.

A data warehouse migration project involves many components. These include schema, data, extract-transform-load (ETL) pipelines, authorization privileges, users, BI tool semantic access layers, and analytic applications.

After your data warehouse has been migrated to Azure Synapse Analytics, you can take advantage of other technologies in the Microsoft analytical ecosystem. Doing so allows you to not only modernize your data warehouse but also bring together insights produced in other analytical data stores on Azure.

You can broaden ETL processing to ingest data of any type into Azure Data Lake Storage. You can prepare and integrate it at scale by using Azure Data Factory. This produces trusted, commonly understood data assets that can be consumed by your data warehouse, and also accessed by data scientists and other applications. You can build real-time, batch-oriented analytical pipelines. You can also create machine learning models that can deploy to run in batch, in real time on streaming data, and on demand.

In addition, you can use PolyBase to go beyond your data warehouse. This simplifies access to insights being produced in multiple underlying analytical platforms on Azure. You create holistic, integrated views in a logical data warehouse to gain access to streaming, big data, and traditional data warehouse insights from BI tools and applications.

Many companies have had data warehouses running in their datacenters for years, to enable users to produce business intelligence. Data warehouses extract data from known transaction systems, stage the data, and then clean, transform, and integrate it to populate data warehouses.

Use cases, business cases, and technology advances all support how Azure Synapse Analytics can help you with data warehouse migration. The following sections list many of these examples.

## Use cases

- Connected product innovation
- Factory of the future
- Clinical analytics
- Compliance analytics
- Cost-based analytics
- Omni-channel optimization
- Personalization
- Intelligent supply chain
- Dynamic pricing
- Procurement analytics

- Digital control tower
- Risk management
- Customer analytics
- Fraud detection
- Claims analytics

## Business cases

- Build end-to-end analytics solutions with a single analytics service.
- Use the Azure Synapse Analytics studio, which provides a unified workspace for data prep, data management, data warehousing, big data, and AI tasks.
- Build and manage pipeline with a no-code visual environment, automate query optimization, build proofs of concept, and use Power BI, all from the same analytics service.
- Deliver your data insights to data warehouses and big data analytics systems.
- For mission-critical workloads, optimize the performance of all queries with intelligent workload management, workload isolation, and limitless concurrency.
- Edit and build Power BI dashboards directly from Azure Synapse Analytics.
- Reduce project development time for BI and machine learning projects.
- Easily share data with just a few clicks by using Azure Data Share integration within Azure Synapse Analytics.
- Implement fine-grained access control with column-level security and native row-level security.
- Automatically protect sensitive data in real time with dynamic data masking.
- Industry-leading security with built-in security features like automated threat detection and always-on data encryption.

## Technology advances

- No hardware to buy or maintenance costs so you pay only for what you use.
- No infrastructure to manage, so you can focus on competitive insights.
- Massively parallel SQL query processing with dynamic scalability when you need it, and the option to shut down or pause when you don't.
- Ability to independently scale storage from compute.
- You can avoid unnecessary, expensive upgrades caused by the staging areas on your data warehouse getting too big, taking up storage capacity, and forcing an upgrade. For example, move the staging area to Azure Data Lake Storage. Then process it with an ETL tool like Azure Data Factory or your existing ETL tool running on Azure at lower cost.
- Avoid expensive hardware upgrades by processing ETL workloads in Azure, by using Azure Data Lake Storage and Azure Data Factory. This is often a better solution than running on your existing data warehouse DBMS with SQL query processing doing the work. As staging data volumes increase, more storage and compute power underpinning your on-premises data warehouse is consumed by ETL. This in turn affects the performance of query, reporting, and analysis workloads.
- Avoid building expensive data marts that use storage and databases software licenses on on-premises hardware. You can build them in Azure Synapse Analytics instead. This is especially helpful if your data warehouse is a Data Vault design, which often causes an increased demand for data marts.
- Avoid the cost of analyzing and storing high-velocity, high-volume data on on-premises hardware. For example, if you need to analyze real-time, machine generated data like click-stream and streaming IoT data in your data warehouse, you can use Azure Synapse Analytics.
- You can avoid paying a premium for storing data on expensive warehouse hardware in the datacenter as your data warehouse grows. Azure Synapse Analytics can store your data in cloud storage at a lower cost.

## Next steps

[Data democratization](#)

# Data democratization

11/9/2020 • 2 minutes to read • [Edit Online](#)

Many companies keep data warehouses in their datacenters to help different parts of their business analyze data and make decisions. Sales, marketing, and finance departments rely heavily on these systems in order to produce standard reports and dashboards. Companies also employ business analysts to perform ad hoc querying and analysis of data in data marts. These data marts use self-service business intelligence tools to perform multidimensional analysis.

A business that's supported by data innovation and a modern data estate can empower a broad range of contributors, from an IT stakeholder to a data professional and beyond. They can take action on this repository of centralized data, which is often referred to as "the single source of truth."

Azure Synapse Analytics is a single service for seamless collaboration and accelerated time-to-insight. To understand this service in more detail, first consider the various roles and skills involved in a typical data estate:

**Data warehousing:** *database admins* support the management of data lakes and data warehouses, while intelligently optimizing workloads and automatically securing data.

**Data integration:** *data engineers* use a code-free environment to easily connect multiple sources and types of data.

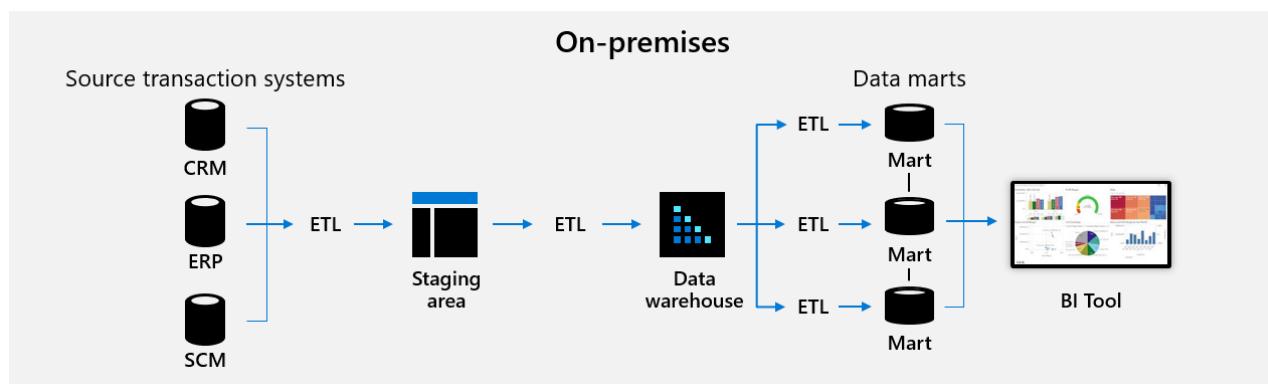
**Big data and machine learning:** *data scientists* build proofs of concept rapidly and provision resources as needed, while working in the language of their choice (for example, T-SQL, Python, Scala, .NET, or Spark SQL).

**Management and security:** *IT pros* protect and manage data more efficiently, enforce privacy requirements, and secure access to cloud and hybrid configurations.

**Business intelligence:** *business analysts* securely access datasets, build dashboards, and share data within and outside their organization.

The following diagram shows an example of a classic data warehouse architecture. Known structured data is extracted from core transaction processing systems and copied into a staging area. From there, it's cleaned, transformed, and integrated into production tables in a data warehouse. It's often the case that several years of historical transaction data are incrementally built up here. This provides the data needed to understand changes in sales, customer purchasing behavior, and customer segmentation over time. It also provides yearly financial reporting and analysis to help with decision making.

From there, subsets of data are extracted into data marts to analyze activity associated with a specific business process. This supports decision making in a specific part of the business.



For a business to run efficiently, it needs all types of data for the different skills and roles described earlier. You need

raw data that has been cleansed for data scientists to build machine-learning models. You need cleaned and structured data for a data warehouse to provide reliable performance to business applications and dashboards. Most importantly, you need to be able to go from raw data to insights in minutes, not days.

Azure Synapse Analytics has a native, built-in business intelligence tool with Power BI. This fully enables you to go from raw data to a dashboard serving insights in minutes, by using one service within one single interface.

# Examples of fiscal outcomes

11/9/2020 • 7 minutes to read • [Edit Online](#)

At the top level, fiscal conversations consist of three basic concepts:

- **Revenue:** Will more money come into the business as a result of the sales of goods or services.
- **Cost:** Will less money be spent in the creation, marketing, sales, or delivery of goods or services.
- **Profit:** Although they're rare, some transformations can both increase revenue and decrease costs. This is a profit outcome.

The remainder of this article explains these fiscal outcomes in the context of a cloud transformation.

## NOTE

The following examples are hypothetical and should not be considered a guarantee of returns when adopting any cloud strategy.

## Revenue outcomes

### New revenue streams

The cloud can help create opportunities to deliver new products to customers or deliver existing products in a new way. New revenue streams are innovative, entrepreneurial, and exciting for many people in the business world. New revenue streams are also prone to failure and are considered by many companies to be high risk. When revenue-related outcomes are proposed by IT, there will likely be resistance. To add credibility to these outcomes, partner with a business leader who's a proven innovator. Validation of the revenue stream early in the process helps avoid roadblocks from the business.

- **Example:** A company has been selling books for over a hundred years. An employee of the company realizes that the content can be delivered electronically. The employee creates a device that can be sold in the bookstore, which allows the same books to be downloaded directly, driving  $x\%$  in new book sales.

### Revenue increases

With global scale and digital reach, the cloud can help businesses to increase revenues from existing revenue streams. Often, this type of outcome comes from an alignment with sales or marketing leadership.

- **Example:** A company that sells widgets could sell more widgets, if the salespeople could securely access the company's digital catalog and stock levels. Unfortunately, that data is only in the company's ERP system, which can be accessed only via a network-connected device. Creating a service façade to interface with the ERP and exposing the catalog list and nonsensitive stock levels to an application in the cloud would allow the salespeople to access the data they need while onsite with a customer. Extending on-premises Active Directory using Azure Active Directory (Azure AD) and integrating role-based access into the application would allow the company to help ensure that the data stays safe. This simple project could affect revenue from an existing product line by  $x\%$ .

### Profit increases

Seldom does a single effort simultaneously increase revenue and decrease costs. However, when it does, align the outcome statements from one or more of the revenue outcomes with one or more of the cost outcomes to communicate the desired outcome.

# Cost outcomes

## Cost reduction

Cloud computing can reduce capital expenses for hardware and software, setting up datacenters, running on-site datacenters, and so on. The costs of racks of servers, round-the-clock electricity for power and cooling, and IT experts for managing the infrastructure add up fast. Shutting down a datacenter can reduce capital expense commitments. This is commonly referred to as "getting out of the datacenter business." Cost reduction is typically measured in dollars in the current budget, which could span one to five years depending on how the CFO manages finances.

- **Example #1:** A company's datacenter consumes a large percentage of the annual IT budget. IT chooses to conduct a cloud migration and transitions the assets in that datacenter to infrastructure as a service (IaaS) solutions, creating a three-year cost reduction.
- **Example #2:** A holding company recently acquired a new company. In the acquisition, the terms dictate that the new entity should be removed from the current datacenters within six months. Failure to do so will result in a fine of \$1 million USD per month to the holding company. Moving the digital assets to the cloud in a cloud migration could allow for a quick decommission of the old assets.
- **Example #3:** An income tax company that caters to consumers experiences 70 percent of its annual revenue during the first three months of the year. The remainder of the year, its large IT investment is relatively dormant. A cloud migration could allow IT to deploy the compute/hosting capacity required for those three months. During the remaining nine months, the IaaS costs could be significantly reduced by shrinking the compute footprint.

### Example: Coverdell

Coverdell modernizes their infrastructure to drive record cost savings with Azure. Coverdell's decision to invest in Azure, and to unite their network of websites, applications, data, and infrastructure within this environment, led to more cost savings than the company could have ever expected. The migration to an Azure-only environment eliminated \$54,000 USD in monthly costs for colocation services. With the company's new united infrastructure alone, coverdell expects to save an estimated \$1M USD over the next two to three years.

"Having access to the Azure technology stack opens the door for some scalable, easy-to-implement, and highly available solutions that are cost effective. This allows our architects to be much more creative with the solutions they provide."

Ryan Sorensen

Director of Application Development and Enterprise Architecture

Coverdell

## Cost avoidance

Terminating a datacenter can also provide cost avoidance, by preventing future refresh cycles. A refresh cycle is the process of buying new hardware and software to replace aging on-premises systems. In Azure, hardware and OS are routinely maintained, patched, and refreshed at no additional cost to customers. This allows a CFO to remove planned future spend from long-term financial forecasts. Cost avoidance is measured in dollars. It differs from cost reduction, generally focusing on a future budget that has not been fully approved yet.

- **Example:** A company's datacenter is up for a lease renewal in six months. The datacenter has been in service for eight years. Four years ago, all servers were refreshed and virtualized, costing the company millions of dollars. Next year, the company plans to refresh the hardware and software again. Migrating the assets in that datacenter as part of a cloud migration would allow cost avoidance by removing the planned refresh from next year's forecasted budget. It could also produce cost reduction by decreasing or eliminating the real estate lease costs.

## Capital expenses and operating expenses

Before you discuss cost outcomes, it's important to understand the two primary cost options: capital expenses and operating expenses.

The following terms will help you understand the differences between capital expenses and operating expenses during business discussions about a transformation journey.

- **Capital** is the money and assets owned by a business to contribute to a particular purpose, such as increasing server capacity or building an application.
- **Capital expenditures** generate benefits over a long period. These expenditures are generally nonrecurring and result in the acquisition of permanent assets. Building an application could qualify as a capital expenditure.
- **Operating expenditures** are ongoing costs of doing business. Consuming cloud services in a pay-as-you-go model could qualify as an operating expenditure.
- **Assets** are economic resources that can be owned or controlled to produce value. Servers, data lakes, and applications can all be considered assets.
- **Depreciation** is a decrease in the value of an asset over time. More relevant to the capital expense versus operating expense conversation, depreciation is how the costs of an asset are allocated across the periods in which they are used. For example, if you build an application this year but it's expected to have an average shelf life of five years (like most commercial applications), the cost of the development team and the tools required to create and deploy the code base would be depreciated evenly over five years.
- **Valuation** is the process of estimating how much a company is worth. In most industries, valuation is based on the company's ability to generate revenue and profit, while respecting the operating costs required to create the goods that provide that revenue. In some industries, such as retail, or in some transaction types, such as private equity, assets and depreciation can play a large part in the company's valuation.

It is often a safe bet that various executives, including the chief investment officer (CIO), debate the best use of capital to grow the company in the desired direction. Giving the CIO a means of converting contentious capital expense conversations into clear accountability for operating expenses could be an attractive outcome by itself. In many industries, chief financial officers (CFOs) are actively seeking ways of better associating fiscal accountability to the cost of goods being sold.

However, before you associate any transformation journey with this type of capital versus operating expense conversion, it's wise to meet with members of the CFO or CIO teams to see which cost structure the business prefers. In some organizations, reducing capital expenses in favor of operating expenses is a highly undesirable outcome. As previously mentioned, this approach is sometimes seen in retail, holding, and private equity companies that place higher value on traditional asset accounting models, which place little value on IP. It's also seen in organizations that had negative experiences when they outsourced IT staff or other functions in the past.

If an operating expense model is desirable, the following example could be a viable business outcome:

- **Example:** The company's datacenter is currently depreciating at  $\$x\ USD$  per year for the next three years. It is expected to require an additional  $\$y\ USD$  to refresh the hardware next year. We can convert the capital expenses to an operating expense model at an even rate of  $\$z\ USD$  per month, allowing for better management of and accountability for the operating costs of technology.

## Next steps

Learn more about [agility outcomes](#).

[Agility outcomes](#)

# Examples of agility outcomes

11/9/2020 • 3 minutes to read • [Edit Online](#)

As discussed in the [business outcomes overview](#), several potential business outcomes can serve as the foundation for any transformation journey conversation with the business. This article focuses on the timeliest business measure: business agility. Understanding your company's market position and competitive landscape can help you articulate the business outcomes that are the target of the business's transformation journey.

Traditionally, chief investment officers and IT teams were considered a source of stability in core mission-critical processes. This is still true. Few businesses can function well when their IT platform is unstable. However, in today's business world, much more is expected. IT can expand beyond a simple cost center by partnering with the business to provide market advantages. Many chief investment officers and executives assume that stability is simply a baseline for IT. For these leaders, business agility is the measure of IT's contribution to the business.

## Why is agility so important?

Markets change at a faster pace today than ever before. As of 2015, only 57 companies were still in the Fortune 500 61 years later—an 88.6 percent turnover rate. This represents market change at a previously unheard-of rate. IT agility or even business agilities are unlikely to affect an organization listing on the Fortune 500, but these figures help us understand the pace at which markets continue to change.

For incumbents and upstarts alike, business agility can be the difference between success or failure of a business initiative. Quickly adapting to market changes can help ring-fence existing customers or claim market share from competitors. The agility-related outcomes in the next sections can help communicate the value of the cloud during a transformation.

## Time-to-market outcome

During cloud-enabled innovation efforts, time to market is a key measure of IT's ability to address market change. In many cases, a business leader might have existing budget for the creation of an application or the launch of a new product. Clearly communicating a time-to-market benefit can motivate that leader to redirect budget to IT's transformation journey.

- **Example 1:** The European division of a US-based company needs to comply with GDPR regulations by protecting customer data in a database that supports UK operations. Their existing version of SQL Server doesn't support the necessary row-level security. An in-place upgrade would be too disruptive. Using Azure SQL Database to replicate and upgrade the database, the customer adds the necessary compliance measure in a matter of weeks.
- **Example 2:** A logistics company has discovered an untapped segment of the market, but it needs a new version of their flagship application to capture this market share. Their larger competitor has made the same discovery. Through the execution of a cloud-enabled application innovation effort, the company embraces customer obsession and a DevOps-driven development approach to beat their slower, legacy competitor by  $x$  months. This jump on market entrance secured the customer base.

### Aurora Health Care

Healthcare system transforms online services into a friendly digital experience. To transform its digital services, Aurora Health Care migrated its websites to the Microsoft Azure platform and adopted a strategy of continuous innovation.

"As a team, we're focused on high-quality solutions and speed. Choosing Azure was a very transformative

decision for us."

Jamey Shiels

Vice President of Digital Experience

Aurora Health Care

## Provision time

When business demands new IT services or scale to existing services, acquisition and provision of new hardware or virtual resources can take weeks. After cloud migration, IT can more easily enable self-service provisioning, allowing the business to scale in hours.

- **Example:** A consumer packaged goods company requires the creation and tear-down of hundreds of database clusters per year to fulfill operational demands of the business. The on-premises virtual hosts can provision quickly, but the process of recovering virtual assets is slow and requires significant time from the team. As such, the legacy on-premises environment suffers from bloat and can seldom keep up with demand. After cloud migration, IT can more easily provide scripted self-provisioning of resources, with a chargeback approach to billing. Together, this allows the business to move as quickly as they need, but still be accountable for the cost of the resources they demand. Doing so in the cloud limits deployments to the business's budget only.

## Next steps

Learn more about [reach outcomes](#).

[Reach outcomes](#)

# Examples of global reach outcomes

11/9/2020 • 3 minutes to read • [Edit Online](#)

As discussed in [Business outcomes](#), several potential business outcomes can serve as the foundation for any transformation journey conversation with the business. This article focuses on a common business measure: reach. *Reach* is a concise term that, in this case, refers to a company's globalization strategy. Understanding the company's globalization strategy helps you better articulate the business outcomes that are the target of a business's transformation journey.

Fortune 500 and smaller enterprises have focused on the globalization of services and customers for over three decades, and most business are likely to engage in global commerce as this globalization continues to pull focus. Hosting datacenters around the world can consume more than 80 percent of an annual IT budget, and wide-area networks using private lines to connect those datacenters can cost millions of dollars per year. Therefore, supporting global operations is both challenging and costly.

Cloud solutions move the cost of globalization to the cloud provider. In Azure, customers can quickly deploy resources in the same region as customers or operations, without buying and provisioning a datacenter. Microsoft owns one of the largest wide-area networks in the world, connecting datacenters around the globe. Connectivity and global operating capacity are available to global customers on demand.

## Global access

Expanding into a new market can be one of the most valuable business outcomes during a transformation. The ability to quickly deploy resources in market without a longer-term commitment allows sales and operations leaders to explore options that wouldn't have been considered in the past.

### Manufacturing example

A cosmetics manufacturer has identified a trend. Some products are being shipped to the Asia Pacific region even though no sales teams are operating in that region. The minimum systems required by a remote sales force are small, but latency prevents a remote access solution. To capitalize on this trend, the vice president of sales wants to experiment with sales teams in Japan and South Korea. Because the company has undergone a cloud migration, it was able to deploy the necessary systems in both Japan and South Korea within days. This allowed the vice president of sales to grow revenue in the region by  $x\%$  within three months. Those two markets continue to outperform other parts of the world, leading to sales operations throughout the region.

### Retail example

An online retailer that ships products globally can engage with their customers across time zones and multiple languages. The retailer uses Azure Bot Service and various features in Azure Cognitive Services, such as Translator, Language Understanding (LUIS), QnA Maker, and Text Analytics. This ensures their customers are able to get the information they need when they need it, and that it's provided to them in their language. The retailer uses the [Personalizer service](#) to further customize the experience and catalog offerings for their customers, ensuring geographical tastes, preferences, and availability are reflected.

## Data sovereignty

Operating in new markets introduces additional governance constraints. Azure provides compliance offerings that help customers meet compliance obligations across regulated industries and global markets. For more information, see the [overview of Microsoft Azure compliance](#).

### Example

A US-based utilities provider was awarded a contract to provide utilities in Canada. Canadian data sovereignty law requires that Canadian data stays in Canada. This company had been working their way through a cloud-enabled application innovation effort for years. As a result, their software was deployed through fully scripted DevOps processes. With a few minor changes to the code base, they were able to deploy a working copy of the code to an Azure datacenter in Canada, meeting data sovereignty compliance and retaining the customer.

## Next steps

Learn more about customer engagement outcomes.

[Customer engagement outcomes](#)

# Examples of customer engagement outcomes

11/9/2020 • 2 minutes to read • [Edit Online](#)

As discussed in the [business outcomes overview](#), several potential business outcomes can serve as the foundation for any transformation journey conversation with the business. This article focuses on a common business measure: customer engagement. Understanding the needs of customers, and the ecosystem around customers, helps you to articulate the business outcomes that are the target of a business's transformation journey.

During cloud-enabled data innovation efforts, you can assume that customers are engaged. The following functions are potentially disruptive and require a high degree of customer engagement:

- Aggregating data
- Testing theories
- Advancing insights
- Informing cultural change

Customer engagement outcomes are about meeting and exceeding customer expectations. As a baseline for customer engagements, customers assume that products and services perform and are reliable. When they're not, it's easy for an executive to understand the business value of performance and reliability outcomes. For more advanced companies, the speed of integrating learnings and observations from this process is a fundamental business outcome.

The next sections provide examples and outcomes related to customer engagement.

## Cycle time

During customer-obsessed transformations such as a cloud-enabled application innovation effort, customers respond from direct engagement. They also appreciate seeing their needs met quickly by the development team. Cycle time is a Six Sigma term that refers to the duration from the start to the finish of a function. For business leaders who invest heavily in improving customer engagement, cycle time can be a strong business outcome.

### Example

A services company that provides business-to-business (B2B) services is trying to retain market share in a competitive market. Customers who have left for a competing service provider found that their overly complex technical solution interferes with their business processes, and is the primary reason for leaving. In this case, cycle time is imperative.

It currently takes 12 months for a feature to progress from request to release. If it's prioritized by the executive team, this cycle can shorten from nine to six months. The team can cut cycle time down to one month through a cloud-enabled application innovation effort, cloud-native application models, and Azure DevOps integration. This frees business and application development teams to interact more directly with customers.

## Intelligent contact center

Customer satisfaction and experience are at the core of successful organizations. Freeing your employees to focus on superior customer service can strongly affect customer loyalty and retention. With the AI technology available today, many steps during a customer call can be automated, enabling the contact center agent more time to focus on delivering superior customer service.

### Example

An insurance company has implemented digital agents to respond rapidly to customer requests. These digital

agents are available through the company website and mobile app, by building an Azure Bot Service solution. Extending an enhanced customer service experience to their contact center, the insurance company implemented live call transcription, sentiment analysis, and key phrase detection. These help the contact center agent with recommended next steps and form processing. This led to reduced repetition from the customer calling the contact center, and enabled the contact center agent to focus more on providing a great customer experience.

## Next steps

Learn more about performance outcomes.

[Performance outcomes](#)

# Examples of performance outcomes

11/9/2020 • 2 minutes to read • [Edit Online](#)

As discussed in [Business outcomes](#), several potential business outcomes can serve as the foundation for any transformation journey conversation with the business. This article focuses on a common business measure: performance.

In today's technological society, customers assume that applications will perform well and always be available. When this expectation isn't met, it causes reputation damage that can be costly and long-lasting.

## Performance

The biggest cloud computing services run on a worldwide network of secure datacenters, which are regularly upgraded to the latest generation of fast and efficient computing hardware. This provides several benefits over a single corporate datacenter, such as reduced network latency for applications and greater economies of scale.

Transform your business and reduce costs with an energy-efficient infrastructure that spans more than 100 highly secure facilities worldwide, linked by one of the largest networks on earth. Azure has more global regions than any other cloud provider. This translates into the scale that's required to bring applications closer to users around the world, preserve data residency, and provide comprehensive compliance and resiliency options for customers.

- **Example 1:** A services company worked a hosting provider that hosted multiple operational infrastructure assets. Those systems suffered from frequent outages and poor performance. The company migrated its assets to Azure to take advantage of the SLA and performance controls of the cloud. Any downtime would cost the company approximately \$15,000 USD per minute of outage. With between four and eight hours of outage per month, it was easy to justify this organizational transformation.
- **Example 2:** A consumer investment company was in the early stages of a cloud-enabled application innovation effort. Agile processes and DevOps were maturing well, but application performance was spiky. As a more mature transformation, the company started a program to monitor and automate sizing based on usage demands. The company eliminated sizing issues by using Azure performance management tools, resulting in a surprising five-percent increase in transactions.

## Reliability

Cloud computing makes data backup, disaster recovery, and business continuity easier and less expensive, because data can be mirrored at multiple redundant sites on the cloud provider's network.

One of IT's crucial functions is ensuring that corporate data is never lost and applications stay available despite server crashes, power outages, or natural disasters. You can keep your data safe and recoverable by backing it up to Azure.

Azure Backup is a simple solution that decreases your infrastructure costs while providing enhanced security mechanisms to protect your data against ransomware. With one solution, you can protect workloads that are running in Azure and on-premises across Linux, Windows, VMware, and Hyper-V. You can ensure business continuity by keeping your applications running in Azure.

Azure Site Recovery makes it simple to test disaster recovery by replicating applications between Azure regions. You can also replicate on-premises VMware and Hyper-V virtual machines and physical servers to Azure to stay available if the primary site goes down. And you can recover workloads to the primary site when it's up and running again.

- **Example:** An oil and gas company used Azure technologies to implement a full site recovery. The company chose not to fully embrace the cloud for day-to-day operations, but the cloud's business continuity and disaster recovery (BCDR) features still protected their datacenter. As a hurricane formed hundreds of miles away, their implementation partner started recovering the site to Azure. Before the hurricane touched down, all mission-critical assets were running in Azure, preventing any downtime.

## Next steps

Learn how to use the business outcome template.

[Use the business outcome template](#)

# Sustainability outcomes and benefits for business

11/9/2020 • 2 minutes to read • [Edit Online](#)

Though the impact and benefits of the cloud have been traditionally measured with financial and efficiency metrics, it's become more common for customers to seek understanding about how the cloud can help them to achieve their sustainability and environmental goals. Cloud computing can support your organization to reduce carbon emissions, use resources more efficiently, and lessen your environmental footprint.

Microsoft has been leading in many of these areas. The company has been operating as carbon-neutral since 2012 and has made a commitment to be carbon-negative by 2030. [The carbon benefits of cloud computing](#), a study on the Microsoft cloud in partnership with WSP, supports research on how moving on-premises datacenters to the Microsoft cloud can significantly reduce carbon footprints.

## The Microsoft sustainability journey

The Microsoft journey started over a decade ago when the company started to apply new business practices and adopt cloud technology. We lowered our carbon emissions by 30 percent in 2009. Since then, Microsoft has made large strides forward by investing in reducing the company's carbon footprint further. Microsoft has focused on these four areas:

- **Carbon:** Cutting energy consumption across corporate offices, charging carbon tax to business divisions, and using cloud-powered technology to lower emissions.
- **Ecosystem:** Making a commitment to green datacenters and purchasing of 1.1 billion kilowatt-hours of green energy.
- **Water:** Reducing use intensity and investing in technology for managing water.
- **Waste:** Practicing responsible sourcing, recycling, and disposal; using software and technology to make buildings more efficient.

Read more about how the Microsoft [commitment to a planet-sized challenge](#) has helped us plan and achieve sustainability goals.

## Examples of sustainability outcomes

Focusing on sustainability and protecting limited environmental resources is key to our future, and this focus also benefits business. Today, companies can draw from a broad range of assets and resources that can help them to expand into new geographic areas and develop innovative resource management solutions.

AGL, one of Australia's leading integrated energy companies, built a solution on Azure that remotely manages networked solar batteries. Learn about how the company is [growing an innovative energy partnership across Australia](#) to help local customers give back to the grid.

Bee'ah is a sustainability pioneer in the middle east that believes in technology and sustainability creating solutions for the future. Their services include waste management, environmental consulting, renewable energy, and sustainable transportation. Azure has supported the company to launch the first AI platform to digitize all operations and services. Read more about how the [cloud drives sustainable management and digital innovation](#) throughout the company's sustainability journey.

These customer stories demonstrate how prioritizing sustainability and environmental solutions can help organizations to create new business opportunities.

## Next steps

An intentional approach can help organizations to navigate their sustainability journey. These four steps can influence outcomes for your company:

**Step 1:** Record and understand your company's carbon emissions. Start by categorizing your emissions, which will help you to list of areas on which to focus. The [Microsoft sustainability calculator](#) can assist you with this task.

**Step 2:** Evaluate whether your vendors, partners, and providers are taking steps to reduce their emissions and if these steps align with yours.

**Step 3:** Create an incentive for teams to reduce carbon emissions. [The Microsoft carbon fee: Theory and practice](#) can help your organization to drive alignment and accountability across your teams.

**Step 4:** Seek out teams in our business to enlist their support and generate ideas for areas for improvement. Build an innovation culture where individuals are participants with a sense of ownership.

Learn more about how your organization can [measure](#) and [reach](#) sustainability outcomes with the cloud.

[Reach outcomes](#)

# How to use the business outcome template

11/9/2020 • 2 minutes to read • [Edit Online](#)

As discussed in the [business outcomes overview](#), it can be difficult to bridge the gap between business and technical conversations. This simple template is designed to help teams uniformly capture business outcomes to be used later in the development of customer transformation journey strategies.

Download the [business outcome template](#) to begin brainstorming and tracking business outcomes. Continue reading to learn how to use the template. Review the [business outcomes section](#) for ideas on potential business outcomes that could come up in executive conversations.

## Use the business outcome template

In this template, business outcomes focus on three topics:

- Aligning to stakeholders or business decision makers.
- Understanding business drivers and objectives.
- Mapping outcomes to specific solutions and technical capability.

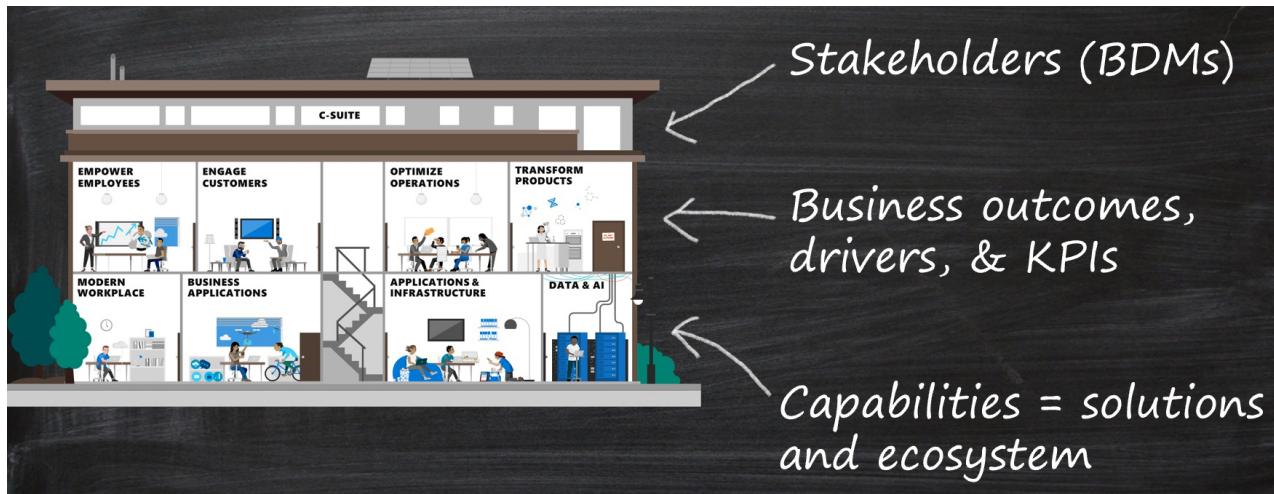


Figure 1: Business outcomes visualized as a house with stakeholders, over business outcomes, over technical capabilities.

The business outcome template focuses on simplified conversations that can quickly engage stakeholders without getting too deep into the technical solution. By rapidly understanding and aligning the key performance indicators (KPIs) and business drivers that are important to stakeholders, your team can think about high-level approaches and transformations before diving into the implementation details.

An example can be found on the "example outcome" tab of the spreadsheet, as shown below. To track multiple outcomes, add them to the "collective outcomes" tab.

XYZ Life Sciences Co. - Drug & Device Division		
Stakeholder:	Business Outcome:	
Business Drivers	KPI	Capabilities
Study Design	\$3M opportunity cost per day per drug	Data-Driven protocol authoring
Study Conduct		Trial Simulation
		Structured collaboration for trial approval

Figure 2: Example of a business outcome template.

## Why is this template relevant?

Discovery is a fundamental tenet of enterprise architecture. If discovery is limited to technical discovery, the solution is likely to miss many opportunities to improve the business. Enterprise architects, solution architects, and other technically minded leaders can master the discovery process by using this template. In effective discovery processes, these leaders consider five key aspects of the business outcome before leading a transformation journey, as shown in the following image:

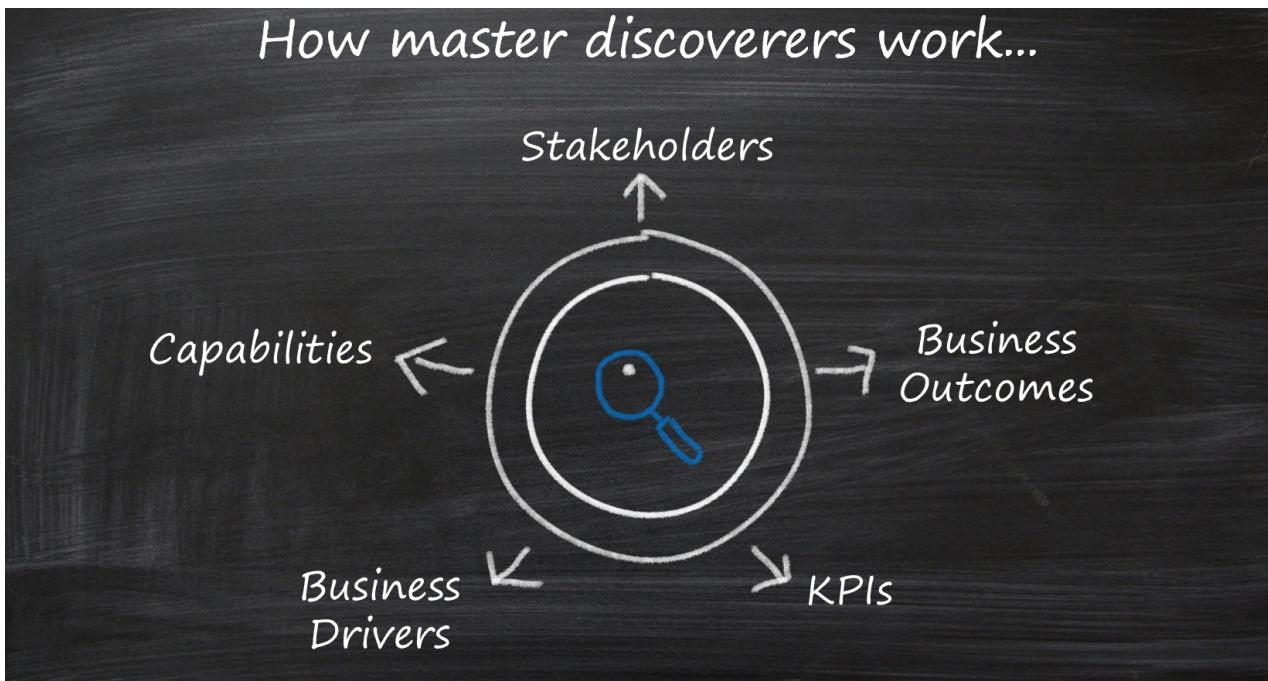


Figure 3: Five areas of focus in discovery: stakeholders, outcomes, drivers, KPIs, and capabilities.

**Stakeholders:** Who in the organization is likely to see the greatest value in a specific business outcome? Who is most likely to support this transformation, especially when things get tough or time consuming? Who has the greatest stake in the success of this transformation? This person is a potential stakeholder.

**Business outcomes:** A business outcome is a concise, defined, and observable result or change in business performance, supported by a specific measure. How does the stakeholder want to change the business? How will the business be affected? What is the value of this transformation?

**Business drivers:** Business drivers capture the current challenge that's preventing the company from achieving desired outcomes. They can also capture new opportunities that the business can capitalize on with the right solution. How would you describe the current challenges or future state of the business? What business functions would be changing to meet the desired outcomes?

**KPIs:** How will this change be measured? How does the business know whether they are successful? How frequently will this KPI be observed? Understanding each KPI helps enable incremental change and experimentation.

**Capabilities:** When you define any transformation journey, how will technical capabilities accelerate realization of the business outcome? What applications must be included in the transformation to achieve business objectives? How do various applications or workloads get prioritized to deliver on capabilities? How do parts of the solution need to be expanded or rearchitected to meet each of the outcomes? Can execution approaches (or timelines) be rearranged to prioritize high-impact business outcomes?

## Next steps

Learn to align your technical efforts to meaningful learning metrics.

[Align your technical efforts](#)

# How can we align efforts to meaningful learning metrics?

11/9/2020 • 3 minutes to read • [Edit Online](#)

The [business outcomes overview](#) discussed ways to measure and communicate the impact a transformation will have on the business. Unfortunately, it can take years for some of those outcomes to produce measurable results. The board and C-suite are unhappy with reports that show a 0% delta for long periods of time.

Learning metrics are interim, shorter-term metrics that can be tied back to longer-term business outcomes. These metrics align well with a growth mindset and help position the culture to become more resilient. Rather than highlighting the anticipated lack of progress toward a long-term business goal, learning metrics highlight early indicators of success. The metrics also highlight early indicators of failure, which are likely to produce the greatest opportunity for you to learn and adjust the plan.

As with much of the material in this framework, we assume you're familiar with the [transformation journey](#) that best aligns with your desired business outcomes. This article will outline a few learning metrics for each transformation journey to illustrate the concept.

## Cloud migration

This transformation focuses on cost, complexity, and efficiency, with an emphasis on IT operations. The most easily measured data behind this transformation is the movement of assets to the cloud. In this kind of transformation, the digital estate is measured by virtual machines (VMs), racks or clusters that host those VMs, datacenter operational costs, required capital expenses to maintain systems, and depreciation of those assets over time.

As VMs are moved to the cloud, dependence on on-premises legacy assets is reduced. The cost of asset maintenance is also reduced. Unfortunately, businesses can't realize the cost reduction until clusters are deprovisioned and datacenter leases expire. In many cases, the full value of the effort isn't realized until the depreciation cycles are complete.

Always align with the CFO or finance office before making financial statements. However, IT teams can generally estimate current monetary cost and future monetary cost values for each VM based on CPU, memory, and storage consumed. You can then apply that value to each migrated VM to estimate the immediate cost savings and future monetary value of the effort.

## Application innovation

Cloud-enabled application innovation focuses largely on the customer experience and the customer's willingness to consume products and services provided by the company. It takes time for increments of change to affect consumer or customer buying behaviors. But application innovation cycles tend to be much shorter than they are in the other forms of transformation. The traditional advice is that you should start with an understanding of the specific behaviors that you want to influence and use those behaviors as the learning metrics. For example, in an e-commerce application, total purchases or add-on purchases could be the target behavior. For a video company, time watching video streams could be the target.

Customer behavior metrics can easily be influenced by outside variables, so it's often important to include related statistics with the learning metrics. These related statistics can include release cadence, bugs resolved per release, code coverage of unit tests, number of page views, page throughput, page load time, and other application performance metrics. Each can show different activities and changes to the code base and the customer experience to correlate with higher-level customer behavior patterns.

## Data innovation

Changing an industry, disrupting markets, or transforming products and services can take years. In a cloud-enabled data innovation effort, experimentation is key to measuring success. Be transparent by sharing prediction metrics like percent probability, number of failed experiments, and number of models trained. Failures will accumulate faster than successes. These metrics can be discouraging, and the executive team must understand the time and investment needed to use these metrics properly.

On the other hand, some positive indicators are often associated with data-driven learning: centralization of heterogeneous data sets, data ingress, and democratization of data. While the team is learning about the customer of tomorrow, real results can be produced today. Supporting learning metrics could include:

- Number of models available.
- Number of partner data sources consumed.
- Devices producing ingress data.
- Volume of ingress data.
- Types of data.

An even more valuable metric is the number of dashboards created from combined data sources. This number reflects the current-state business processes that are affected by new data sources. By sharing new data sources openly, your business can take advantage of the data by using reporting tools like Power BI to produce incremental insights and drive business change.

## Next steps

After learning metrics are aligned, you're ready to begin [building the business case](#) to deliver against those metrics.

[Build the cloud business case](#)

# Measure business outcomes using objectives and key results (OKRs)

11/9/2020 • 3 minutes to read • [Edit Online](#)

Modern operations require modern ways to measure business outcomes, and cloud technology can help to increase velocity for a business. An organization's measurement platform should support a company's outcomes and plan for growth by:

- Providing insights to team members and groups.
- Supporting staff to pivot quickly when outcomes don't align with strategy and expectations.
- Offering a structured format, templates, sequences, and tools to help teams plan and visualize for increasing velocity.

## An overview of objectives and key results (OKRs)

Many organizations have started to adopt objectives and key results (OKRs). OKRs have proven to drive alignment in complex work environments, foster innovation, and help individuals to focus on what matters. The two components comprising OKRs are an objective and key results for that objective. An objective is the statement of intent: what is the team trying to accomplish, and why is it important? Key results are specific outcomes that track impact on the objective.

**Objective:** Clarity and intent.

**Key results:** Measures of success within a quarter.

It's important to understand that OKRs are useful for measuring team outcomes versus individual performance. Since deadlines often motivate team performance, key results are established quarterly. OKRs help teams to focus on the most important tasks instead of the volume of work at hand.

To do this, focus on what happens in a month, a quarter, and other short-term intervals. You can have OKRs that last longer, but shorter intervals emphasize the need for OKRs that track short-term impact.

## OKR key principles

[WorkBoard](#) is a company that focuses solely on OKRs and offers software solutions to help customers adopt them. According to the company, the key principles of OKRs are:

- **Aspire and inspire:** Teams establish their best possible results in a given quarter, focus efforts on great outcomes, and use retros to learn and iterate.
- **Outcome focus:** Quarterly key results provide clarity on where value is created. This helps teams and the organization to drive business impacts faster.
- **Global and local:** Teams localize OKRs into their nouns, verbs, and numbers that enrich OKRs with the team's expertise and insights.
- **Transparent:** OKRs, alignment, and progress are visible to everyone with OKR software, simplifying collaboration and making good decisions faster.

## How OKRs add value to an organization

OKRs help to create alignment and accountability within organizations.

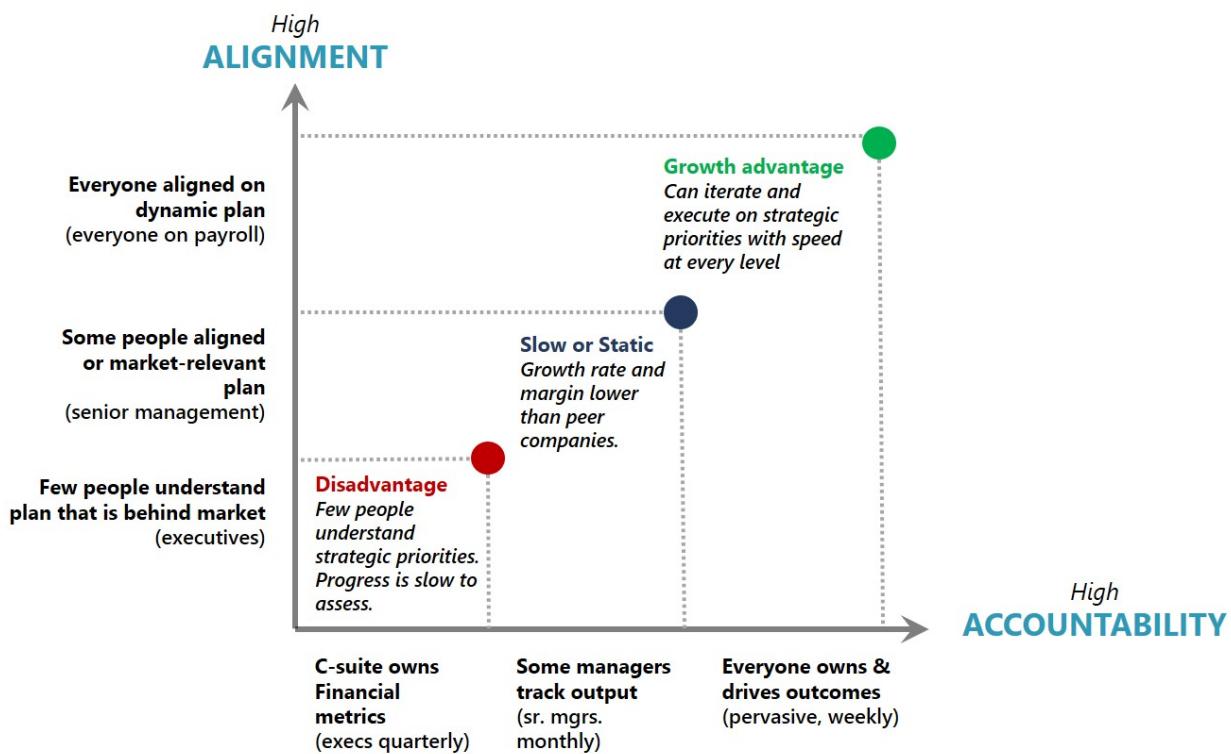


Figure 1: How OKRs increase alignment and accountability within organizations to help them meet goals faster.

Learn more about how your team can align [strategy and execution](#) during planning and execution phases.

## Examples of OKRs

The principles defined by WorkBoard can help your organization to understand how useful OKRs take form. Objectives need to inspire your company and its teams to fully understand your mission. Key results need to be specific and measurable within the quarter.

Here are some example of OKRs:

**Objective 1:** Be the top US provider of learning platforms to schools.

**Key results:**

1. 45 percent of K-12 schools using our platform
2. A 12-percent increase in student engagement, as measured through internal systems
3. A 95-percent satisfaction rate from quarterly parent surveys

**Objective 2:** Build a technology platform that supports every person in our business to innovate and create.

**Key results:**

1. Five new applications developed and adopted across the organization
2. Every team with at least two members using the Microsoft Power Platform
3. Including new cloud technologies like data analytics and machine learning in all customer-facing applications

**Objective 3:** Transform our approach from sales-driven to data-driven.

**Key results:**

1. Increasing pipeline coverage from 50 percent to 200 percent
2. Increasing closing rates for sales engagements by 5 percent
3. Reducing the time to close deals by 8 percent

## Next steps

Five steps can help your organization to move forward with OKRs:

**Step 1: Learn:** Start exploring what OKRs can do for your business, and tune in to some of your industry peers and leaders to learn about how OKRs have benefited their organizations.

**Step 2: Plan:** As you begin to draft your OKRs, ensure that your sponsors are contributing and involved in the process. Work with an OKR coach to refine your OKRs.

**Step 3: Launch:** Each organization launches initiatives differently. Maintain a strong communication plan, and build the OKR calibration and celebration process into your operating model.

**Step 4: Drive:** To maintain rigor and focus, make sure that you're sharing outcomes and results across the organization. This will help your teams to adopt a habit of using OKRs.

**Step 5: Improve:** Continue to improve, revisit, and rethink how to connect further across the organization. OKRs in spreadsheets can be useful, but an organization can benefit most from everyone participating to meet objectives and gaining insights from the aligned data.

Contact [WorkBoard](#) to get started.

[Align efforts for learning metrics](#)

# Build a business justification for cloud migration

11/9/2020 • 8 minutes to read • [Edit Online](#)

Cloud migrations can generate early return on investment (ROI) from cloud transformation efforts. But developing a clear business justification with tangible, relevant costs and returns can be a complex process. This article will help you think about what data you need to create a financial model that aligns with cloud migration outcomes. First, let's dispel a few myths about cloud migration, so your organization can avoid some common mistakes.

## Dispelling cloud migration myths

### **Myth: The cloud is always cheaper**

It's commonly believed that operating a datacenter in the cloud is always cheaper than operating one on-premises. While this assumption might generally be true, it's not always the case. Sometimes cloud operating costs are higher. These higher costs are often caused by poor cost governance, misaligned system architectures, process duplication, atypical system configurations, or greater staffing costs. Fortunately, you can mitigate many of these problems to create early ROI. Following the guidance in [Build the business justification](#) can help you detect and avoid these misalignments. Dispelling the other myths described here can help too.

### **Myth: Everything should go into the cloud**

In fact, some business drivers might lead you to choose a hybrid solution. Before you finalize a business model, it's smart to complete a first-round quantitative analysis, as described in the [digital estate articles](#). For more information about the individual quantitative drivers involved in rationalization, see the [five Rs of rationalization](#). Either approach will use easily obtained inventory data and a brief quantitative analysis to identify workloads or applications that could result in higher costs in the cloud. These approaches could also identify dependencies or traffic patterns that would necessitate a hybrid solution.

### **Myth: Mirroring my on-premises environment will help me save money in the cloud**

During digital estate planning, it's not unheard of for businesses to detect unused capacity of more than 50% of the provisioned environment. If assets are provisioned in the cloud to match current provisioning, cost savings are hard to realize. Consider reducing the size of the deployed assets to align with usage patterns rather than provisioning patterns.

### **Myth: Server costs drive business cases for cloud migration**

Sometimes this assumption is true. For some companies, it's important to reduce ongoing capital expenses related to servers. But it depends on several factors. Companies with a five-year to eight-year hardware refresh cycle are unlikely to see fast returns on their cloud migration. Companies with standardized or enforced refresh cycles can hit a break-even point quickly. In either case, other expenses might be the financial triggers that justify the migration. Here are a few examples of costs that are commonly overlooked when companies take a server-only or VM-only view of costs:

- Costs of software for virtualization, servers, and middleware can be extensive. Cloud providers eliminate some of these costs. Two examples of a cloud provider reducing virtualization costs are the [Azure Hybrid Benefit](#) and [Azure Reservations](#) programs.
- Business losses caused by outages can quickly exceed hardware or software costs. If your current datacenter is unstable, work with the business to quantify the impact of outages in terms of opportunity costs or actual business costs.
- Environmental costs can also be significant. For the average American family, a home is the biggest investment and the highest cost in the budget. The same is often true for datacenters. Real estate, facilities,

and utility costs represent a fair portion of on-premises costs. When datacenters are retired, those facilities can be repurposed, or your business could potentially be released from these costs entirely.

### **Myth: An operating expense model is better than a capital expense model**

As explained in the [fiscal outcomes](#) article, an operating expense model can be a good thing. But some industries view operating expenditures negatively. Here are a few examples that would trigger tighter integration with the accounting and business units regarding the operating expense conversation:

- When a business sees capital assets as a driver for business valuation, capital expense reductions could be a negative outcome. Though it's not a universal standard, this sentiment is most commonly seen in the retail, manufacturing, and construction industries.
- A private equity firm or a company that's seeking capital influx might consider operating expense increases as a negative outcome.
- If a business focuses heavily on improving sales margins or reducing cost of goods sold (COGS), operating expenses could be a negative outcome.

Businesses are more likely to see operating expense as more favorable than capital expense. For example, this approach might be well received by businesses that are trying to improve cash flow, reduce capital investments, or decrease asset holdings.

Before you provide a business justification that focuses on a conversion from capital expense to operating expense, understand which is better for your business. Accounting and procurement can often help align the message to financial objectives.

### **Myth: Moving to the cloud is like flipping a switch**

Migrations are a manually intense technical transformation. When developing a business justification, especially justifications that are time sensitive, consider the following aspects that could increase the time it takes to migrate assets:

- **Bandwidth limitations:** The amount of bandwidth between the current datacenter and the cloud provider will drive timelines during migration.
- **Testing timelines:** Testing applications with the business to ensure readiness and performance can be time consuming. Aligning power users and testing processes is critical.
- **Migration timelines:** The amount of time and effort required to implement the migration can increase costs and cause delays. Allocating employees or contracting partners can also delay the process. The plan should account for these allocations.

Technical and cultural impediments can slow cloud adoption. When time is an important aspect of the business justification, the best mitigation is proper planning. During planning, two approaches can help mitigate timeline risks:

- Invest the time and energy in understanding technical adoption constraints. Though pressure to move quickly might be high, it's important to account for realistic timelines.
- If cultural or people impediments arise, they'll have more serious effects than technical constraints. Cloud adoption creates change, which produces the desired transformation. Unfortunately, people sometimes fear change and might need additional support to align with the plan. Identify key people on the team who are opposed to change and engage them early.

To maximize readiness and mitigation of timeline risks, prepare executive stakeholders by firmly aligning business value and business outcomes. Help those stakeholders understand the changes that will come with the transformation. Be clear and set realistic expectations from the beginning. When people or technologies slow the process, it will be easier to enlist executive support.

## **Build the business justification**

The following process defines an approach to developing the business justification for cloud migrations. For more information about the calculations and financial terms, see the article on [financial models](#).

At the highest level, the formula for business justification is simple. But the subtle data points required to populate the formula can be difficult to align. On a basic level, the business justification focuses on the return on investment (ROI) associated with the proposed technical change. The generic formula for ROI is:

$$\text{Return on Investment (ROI)} = \frac{\text{(Gain from investment} - \text{Initial Investment})}{\text{Initial Investment}}$$

We can unpack this equation to get a migration-specific view of the formulas for the input variables on the right side of the equation. The remaining sections of this article offer some considerations to take into account.

## Migration-specific initial investment

- Cloud providers offer calculators to estimate cloud investments. Microsoft provides the [Azure pricing calculator](#).
- Some cloud providers also offer cost-delta calculators. Microsoft provides the [Azure total cost of ownership \(TCO\) calculator](#).
- For more refined cost structures, consider a [digital estate planning](#) exercise.
- Estimate the cost of migration.
- Estimate the cost of any expected training opportunities. [Microsoft Learn](#) might be able to help mitigate those costs.
- At some companies, the time invested by existing staff members might need to be included in the initial costs. Consult the finance office for guidance.
- Discuss any additional costs or burden costs with the finance office for validation.

## Migration-specific revenue deltas

This aspect is often overlooked by strategists creating a business justification for migration. In some areas, the cloud can cut costs. But the ultimate goal of any transformation is to yield better results over time. Consider the downstream effects to understand long-term revenue improvements. What new technologies will be available to your business after the migration that can't be used today? What projects or business objectives are blocked by dependencies on legacy technologies? What programs are on hold, pending high capital expenditures for technology?

After you consider the opportunities unlocked by the cloud, work with the business to calculate the revenue increases that could come from those opportunities.

## Migration-specific cost deltas

Calculate any changes to costs that will come from the proposed migration. See the [financial models](#) article for details about the types of cost deltas. Cloud providers often offer tools for cost-delta calculations. The [Azure total cost of ownership \(TCO\) calculator](#) is one example.

Other examples of costs that might be reduced by a cloud migration:

- Datacenter termination or reduction (environmental costs)
- Reduction in power consumed (environmental costs)
- Rack termination (physical asset recovery)
- Hardware refresh avoidance (cost avoidance)
- Software renewal avoidance (operational cost reduction or cost avoidance)

- Vendor consolidation (operational cost reduction and potential soft-cost reduction)

## When ROI results are surprising

If the ROI for a cloud migration doesn't match your expectations, you might want to revisit the common myths listed at the beginning of this article.

But it's important to understand that a cost savings isn't always possible. Some applications cost more to operate in the cloud than on-premises. These applications can significantly skew results in an analysis.

When the ROI is below 20%, consider a [digital estate planning](#) exercise, paying specific attention to [rationalization](#). During quantitative analysis, review each application to find workloads that skew the results. It might make sense to remove those workloads from the plan. If usage data is available, consider reducing the size of VMs to match usage.

If the ROI is still misaligned, seek help from your Microsoft sales representative or [engage an experienced partner](#).

## Next steps

[Create a financial model for cloud transformation](#)

# Create a financial model for cloud transformation

11/9/2020 • 5 minutes to read • [Edit Online](#)

Creating a financial model that accurately represents the full business value of any cloud transformation can be complicated. Financial models and business justifications tend to vary for different organizations. This article establishes some formulas and points out a few things that are commonly missed when strategists create financial models.

## Return on investment

Return on investment (ROI) is often an important criteria for the C-suite or the board. ROI is used to compare different ways to invest limited capital resources. The formula for ROI is fairly simple. The details you'll need to create each input to the formula might not be as simple. Essentially, ROI is the amount of return produced from an initial investment. It's usually represented as a percentage:

$$\text{Return on Investment (ROI)} = \frac{\text{(Gain from investment} - \text{Initial Investment)}}{\text{Initial Investment}}$$

In the next sections, we'll walk through the data you'll need to calculate the initial investment and the gain from investment (earnings).

## Calculate initial investment

Initial investment is the capital expense and operating expense required to complete a transformation. The classification of costs can vary depending on accounting models and CFO preference. But this category would include items like professional services to transform, software licenses used only during the transformation, the cost of cloud services during the transformation, and potentially the cost of salaried employees during the transformation.

Add these costs to create an estimate of the initial investment.

## Calculate the gain from investment

Calculating the gain from investment often requires a second formula that's specific to the business outcomes and associated technical changes. Calculating earnings is harder than calculating cost reductions.

To calculate earnings, you need two variables:

$$\text{Gain from Investment} = \text{Revenue Deltas} + \text{Cost Deltas}$$

These variables are described in the following sections.

## Revenue deltas

Revenue deltas should be forecast in partnership with business stakeholders. After the business stakeholders agree on a revenue impact, it can be used to improve the earning position.

# Cost deltas

Cost deltas are the amount of increase or decrease that will be caused by the transformation. Independent variables can affect cost deltas. Earnings are largely based on hard costs like capital expense reductions, cost avoidance, operational cost reductions, and depreciation reductions. The following sections describe some cost deltas to consider.

## Depreciation reduction or acceleration

For guidance on depreciation, speak with the CFO or finance team. The following information is meant to serve as a general reference on the topic of depreciation.

When capital is invested in the acquisition of an asset, that investment could be used for financial or tax purposes to produce ongoing benefits over the expected lifespan of the asset. Some companies see depreciation as a positive tax advantage. Others see it as a committed, ongoing expense similar to other recurring expenses attributed to the annual IT budget.

Speak with the finance office to find out if elimination of depreciation is possible and if it would make a positive contribution to cost deltas.

## Physical asset recovery

In some cases, retired assets can be sold as a source of revenue. This revenue is often lumped into cost reduction for simplicity. But it's truly an increase in revenue and can be taxed as such. Speak with the finance office to understand the viability of this option and how to account for the resulting revenue.

## Operational cost reductions

Recurring expenses required to operate a business are often called operating expenses. This is a broad category. In most accounting models, it includes:

- Software licensing.
- Hosting expenses.
- Electric bills.
- Real estate rentals.
- Cooling expenses.
- Temporary staff required for operations.
- Equipment rentals.
- Replacement parts.
- Maintenance contracts.
- Repair services.
- Business continuity and disaster recovery (BCDR) services.
- Other expenses that don't require capital expense approvals.

This category provides one of the highest earning deltas. When you're considering a cloud migration, time invested in making this list exhaustive is rarely wasted. Ask the CIO and finance team questions to ensure all operational costs are accounted for.

## Cost avoidance

When an operating expenditure is expected but not yet in an approved budget, it might not fit into a cost reduction category. For example, if VMware and Microsoft licenses need to be renegotiated and paid next year, they aren't fully qualified costs yet. Reductions in those expected costs are treated like operational costs for the sake of cost-delta calculations. Informally, however, they should be referred to as "cost avoidance" until negotiation and budget approval is complete.

## Soft-cost reductions

At some companies, soft costs like reductions in operational complexity or reductions in full-time staff for

operating a datacenter could also be included in cost deltas. But including soft costs might not be a good idea. When you include soft-cost reductions, you insert an undocumented assumption that the reduction will create tangible cost savings. Technology projects rarely result in actual soft-cost recovery.

### **Headcount reductions**

Time savings for staff are often included under soft-cost reduction. When those time savings map to actual reduction of IT salary or staffing, they could be calculated separately as headcount reductions.

That said, the skills needed on-premises generally map to a similar (or higher-level) set of skills needed in the cloud. So people aren't generally laid off after a cloud migration.

An exception occurs when operational capacity is provided by a third party or a managed services provider (MSP). If IT systems are managed by a third party, the operating costs could be replaced by a cloud-native solution or cloud-native MSP. A cloud-native MSP is likely to operate more efficiently and potentially at a lower cost. If that's the case, operational cost reductions belong in the hard-cost calculations.

### **Capital expense reductions or avoidance**

Capital expenses are slightly different from operating expenses. Generally, this category is driven by refresh cycles or datacenter expansion. An example of a datacenter expansion would be a new high-performance cluster to host a big data solution or data warehouse. This expense would generally fit into a capital expense category. More common are the basic refresh cycles. Some companies have rigid hardware refresh cycles, meaning assets are retired and replaced on a regular cycle (usually every three, five, or eight years). These cycles often coincide with asset lease cycles or the forecasted life span of equipment. When a refresh cycle hits, IT draws capital expense to acquire new equipment.

If a refresh cycle is approved and budgeted, the cloud transformation could help eliminate that cost. If a refresh cycle is planned but not yet approved, the cloud transformation could avoid a capital expenditure. Both reductions would be added to the cost delta.

## **Next steps**

Learn more about [cloud accounting](#) models.

[Cloud accounting](#)

# What is cloud accounting?

11/9/2020 • 4 minutes to read • [Edit Online](#)

The cloud changes how IT accounts for costs, as is described in [Create a financial model for cloud transformation](#). Various IT accounting models are much easier to support because of how the cloud allocates costs. So it's important to understand how to account for cloud costs before you begin a cloud transformation journey. This article outlines the most common cloud accounting models for IT.

## Traditional IT accounting (cost center model)

It's often accurate to consider IT a cost center. In the traditional IT accounting model, IT consolidates purchasing power for all IT assets. As we pointed out in the [financial models](#) article, that purchasing power consolidation can include software licenses, recurring charges for CRM licensing, purchase of employee desktops, and other large costs.

When IT serves as a cost center, the perceived value of IT is largely viewed through a procurement management lens. This perception makes it difficult for the board or other executives to understand the true value that IT provides. Procurement costs tend to skew the view of IT by outweighing any other value added by the organization. This view explains why IT is often lumped into the responsibilities of either the chief financial officer or the chief operating officer. This perception of IT is limited and might be shortsighted.

## Central IT accounting (profit center model)

To overcome the cost center view of IT, some CIOs opted for a centralized IT model of accounting. In this type of model, IT is treated like a competing business unit and a peer to revenue-producing business units. In some cases, this model can be entirely logical. For example, some organizations have a professional IT services division that generates a revenue stream. Frequently, centralized IT models don't generate significant revenue, making it difficult to justify the model.

Regardless of the revenue model, centralized IT accounting models are unique because of how the IT unit accounts for costs. In a traditional IT model, the IT team records costs and pays those costs from shared funds like operations and maintenance (O&M) or a dedicated profit and loss (P&L) account.

In a central IT accounting model, the IT team marks up the services provided to account for overhead, management, and other estimated expenses. It then bills the competing business units for the marked-up services. In this model, the CIO is expected to manage the P&L associated with the sale of those services. This can create inflated IT costs and contention between central IT and business units, especially when IT needs to cut costs or isn't meeting agreed-upon SLAs. During times of technology or market change, any new technology would cause a disruption to central IT's P&L, making transformation difficult.

## Chargeback

One of the common first steps in changing IT's reputation as a cost center is implementing a chargeback model of accounting. This model is especially common in smaller enterprises or highly efficient IT organizations. In the chargeback model, any IT costs that are associated with a specific business unit are treated like an operating expense in that business unit's budget. This practice reduces the cumulative cost effects on IT, allowing business values to show more clearly.

In a legacy on-premises model, chargeback is difficult to realize because someone still has to carry the large capital expenses and depreciation. The ongoing conversion from capital expenditures to operating expenses associated with usage is a difficult accounting exercise. This difficulty is a major reason for the creation of the

traditional IT accounting model and the central IT accounting model. The operating expenses model of cloud cost accounting is almost required if you want to efficiently deliver a chargeback model.

But you shouldn't implement this model without considering the implications. Here are a few consequences that are unique to a chargeback model:

- Chargeback results in a massive reduction of the overall IT budget. For IT organizations that are inefficient or require extensive complex technical skills in operations or maintenance, this model can expose those expenses in an unhealthy way.
- Loss of control is a common consequence. In highly political environments, chargeback can result in loss of control and staff being reallocated to the business. This could create significant inefficiencies and reduce IT's ability to consistently meet SLAs or project requirements.
- Difficulty accounting for shared services is another common consequence. If the organization has grown through acquisition and is carrying technical debt as a result, it's likely that a high percentage of shared services must be maintained to keep all systems working together effectively.

Cloud transformations include solutions to these and other consequences associated with a chargeback model. But each of those solutions includes implementation and operating expenses. The CIO and CFO should carefully weigh the pros and cons of a chargeback model before considering one.

## Showback or awareness-back

For larger enterprises, a showback or awareness-back model is a safer first step in the transition from cost center to value center. This model doesn't affect financial accounting. In fact, the P&Ls of each organization don't change. The biggest shift is in mindset and awareness. In a showback or awareness-back model, IT manages the centralized, consolidated buying power as an agent for the business. In reports back to the business, IT attributes any direct costs to the relevant business unit, which reduces the perceived budget directly consumed by IT. IT also plans budgets based on the needs of the associated business units, which allows IT to more accurately account for costs associated to purely IT initiatives.

This model provides a balance between a true chargeback model and more traditional models of IT accounting.

## Impact of cloud accounting models

The choice of accounting models is crucial in system design. The choice of accounting model can affect subscription strategies, naming standards, tagging standards, and policy and blueprint designs.

After you've worked with the business to make decisions about a cloud accounting model and [global markets](#), you have enough information to [choose your first cloud adoption project](#).

[Choose your first cloud adoption project](#)

# Strategy for partner alignment

11/9/2020 • 5 minutes to read • [Edit Online](#)

The Cloud Adoption Framework approaches cloud adoption as a self-service activity. The objective is to empower each of the teams supporting adoption through standardized approaches. In practice, you can't assume that a self-service approach will be sufficient for all adoption activities.

Successful cloud adoption programs typically involve at least one level of support. Some cloud adoption efforts may require support from multiple partners working together towards a common goal.

## Steps to align the partnership strategy

During the Strategy phase of adoption, it's important to start aligning your partnership strategy. The following steps can help remove roadblocks in later phases of the adoption lifecycle.

1. Start to understand support needs.
2. Consider partnership options that fit your culture and needs.
3. Evaluate a shortlist of partner options.
4. Begin contract and paperwork reviews with selected partners.

Completing these steps early, will ensure success of the team when the technical efforts begin. The following sections of this article provide guidance for each of these steps.

## Understanding support needs

Throughout the cloud adoption lifecycle, the various teams may require support to be successful. The following are a few examples of the types of help commonly required.

- **Strategy:** Support defining the business strategy and supporting technology strategy.
- **Plan:** Support with discovery of the portfolio, quantitative assessment of the digital estate, development of a cloud adoption plan, creation of a skilling plan.
- **Ready:** Support deploying a landing zone or full cloud environment capable of supporting the cloud adoption plan.
- **Migrate:** Assistance migrating workloads or building a migration factory to ensure sound migration processes.
- **Innovate:** Assistance developing new solutions or rebuilding/rearchitecting existing solutions to drive innovation.
- **Govern:** Support or ongoing managed services to provide governance and controls across the cloud environment.
- **Manage:** Support or ongoing managed services to operate the cloud platform and the workloads hosted in the cloud.

Few corporations have the diversity of skills required to support strategy, planning, readiness, adoption, governance, and management. Partners and other support models are often necessary to fill in the gaps in the team's skills and responsibilities.

Various partnership options can help develop needed skills, augment staffing requirement, or completely offload specific processes.

## Partnership options

You are not alone in your cloud journey. There are several options to support your team throughout your cloud adoption journey.

- **Azure solution providers (partners):** Get connected with Azure expert managed services providers (MSP) and other Microsoft partners who have service offerings aligned to the Cloud Adoption Framework methodologies.
- **FastTrack for Azure:** Use the Microsoft FastTrack for Azure program to accelerate migration.
- **Azure Migration Program (AMP):** The AMP program aligns a mixture of partners and Microsoft employees to accelerate and support your migration.

### Azure solution providers

Microsoft certified solution providers specialize in providing modern customer solutions base on Microsoft technologies across the world. Optimize your business in the cloud with help from an experienced partner.

**Find a Cloud Solution Provider (CSP).** A certified CSP can help take full advantage of the cloud by assessing business goals for cloud adoption, identifying the right cloud solution that meets business needs and helps the business become more agile and efficient.

Azure expert managed services providers (MSP) have undergone a third-party audit to validate a higher tier of capability, demonstrated through certified staff headcounts, customer references, annual consumption of Azure at scale, and other criteria.

**Find a managed service partner.** An Azure managed service partner (MSP) helps a business transition to Azure by guiding all aspects of the cloud journey. From consulting to migrations and operations management, cloud MSPs show customers all the benefits that come with cloud adoption. They also act as a one-stop shop for common support, provisioning, and the billing experience, all with a flexible pay-as-you-go business model.

In parallel to the development of the cloud adoption strategy, the cloud strategy team should start to identify solution providers that can partner in the delivery of business objectives.

### FastTrack for Azure

**FastTrack for Azure** provides direct assistance from Azure engineers, working hand in hand with partners, to help customers build Azure solutions quickly and confidently. FastTrack brings best practices and tools from real customer experiences to guide customers from setup, configuration, and development to production of Azure solutions, including:

During a typical FastTrack for Azure engagement, Microsoft helps to define the business vision to plan and develop Azure solutions successfully. The team assesses architectural needs and provides guidance, design principles, tools, and resources to help build, deploy, and manage Azure solutions. The team matches skilled partners for deployment services on request and periodically checks in to ensure that deployment is on track and to help remove blockers.

### Azure Migration Program (AMP)

The [Azure Migration Program \(AMP\)](#) provides a mixture of technical skill building, step-by-step guidance, free migration tools, and potential offers to reduce migration costs.

The program uses FastTrack for Azure and Azure solution providers to improve customer success during migration.

Watch this short video to get an overview of how the Azure Migration Program can help you.

### Azure support

If you have questions or need help, [create a support request](#). If your support request requires deep technical guidance, visit [Azure support plans](#) to align the best plan for your needs.

## Shortlist of partner options

During strategy development, it's hard to define specific partnership needs. During development of the cloud adoption plan and skilling plan, those needs will come into focus.

But, based on the culture and maturity of your team, it may be possible to decide on a partnership option that is more aligned with your expected needs.

Choose one or more of the partnership options above to narrow down the options to investigate first.

## Begin contract and paperwork reviews

As the shortlist of options is reviewed, there will likely be one or more partners that stand out. If there is a clear leader among the partners, start the process to review contracts and paperwork with the partner.

The contracting process can take time. Reviewing legal terms ahead of time can remove one barrier to engagement when your teams need help the most.

This is especially true if your company requires vendors to be added to an approved vendor list.

## Next steps

After your partner alignment strategy is kicked off, you may want to consider your [security strategy](#) next.

[Define your security strategy](#)

# First cloud adoption project

11/9/2020 • 3 minutes to read • [Edit Online](#)

There's a learning curve and a time commitment associated with cloud adoption planning. Even for experienced teams, proper planning takes time: time to align stakeholders, time to collect and analyze data, time to validate long-term decisions, and time to align people, processes, and technology. In the most productive adoption efforts, planning grows in parallel with adoption, improving with each release and with each workload migration to the cloud. It's important to understand the difference between a cloud adoption plan and a cloud adoption strategy. You need a well-defined strategy to facilitate and guide the implementation of a cloud adoption plan.

The Cloud Adoption Framework for Azure outlines the processes for cloud adoption and the operation of workloads hosted in the cloud. Each of the processes across the Strategy, Plan, Ready, Adopt, and Manage methodologies require slight expansions of technical, business, and operational skills. Some of those skills can come from directed learning. But many of them are most effectively acquired through hands-on experience.

Starting a first adoption process in parallel with the development of the plan provides some benefits:

- Establish a growth mindset to encourage learning and exploration.
- Provide an opportunity for the team to develop necessary skills.
- Create situations that encourage new approaches to collaboration.
- Identify skill gaps and potential partnership needs.
- Provide tangible inputs to the plan.

## First project criteria

Your first adoption project should align with your [motivations](#) for cloud adoption. Whenever possible, your first project should also demonstrate progress toward a defined [business outcome](#).

## First project expectations

Your team's first adoption project is likely to result in a production deployment of some kind. But this isn't always the case. Establish proper expectations early. Here are a few wise expectations to set:

- This project is a source of learning.
- This project might result in production deployments, but it will probably require additional effort first.
- The output of this project is a set of clear requirements to provide a longer-term production solution.

## First project examples

To support the preceding criteria, this list provides an example of a first project for each motivation category:

- **Critical business events:** When a critical business event is the primary motivation, implementation of a tool like [Azure Site Recovery](#) might be a good first project. During migration, you would use a tool like [Azure Migrate](#) to quickly migrate datacenter assets. But during the first project, you could first use Azure Site Recovery as a disaster recovery tool. Reducing dependencies on disaster recovery assets within the datacenter before pragmatically planning the migration.
- **Migration motivations:** When migration is the primary motivation, it's wise to start with the migration of a noncritical workload. The [Azure setup guide](#) and the [Azure migration guide](#) can provide guidance for the migration of your first workload.

- **Innovation motivations:** When innovation is the primary motivation, creation of a targeted dev/test environment can be a great first project.

Additional examples of first adoption projects include:

- **Business continuity and disaster recovery (BCDR):** Beyond Azure Site Recovery, you can implement multiple BCDR strategies as a first project.
- **Nonproduction:** Deploy a nonproduction instance of a workload.
- **Archive:** Cold storage can place a strain on datacenter resources. Moving that data to the cloud is a solid quick win.
- **End of support (EOS):** Migrating assets that have reached the end of support is another quick win that builds technical skills. It could also provide some cost avoidance from expensive support contracts or licensing costs.
- **Virtual desktop interface (VDI):** Creating virtual desktops for remote employees can provide a quick win. In some cases, this first adoption project could also reduce dependence on expensive private networks in favor of commodity public internet connectivity.
- **Dev/test:** Remove dev/test from on-premises environments to give developers control, agility, and self-service capacity.
- **Simple apps (less than five):** Modernize and migrate a simple app to quickly gain developer and operations experience.
- **Performance labs:** When you need high-scale performance in a lab setting, use the cloud to quickly and cost-effectively provision those labs for a short time.
- **Data platform:** Creating a data lake with scalable compute for analytics, reporting, or machine learning workloads, and migrating to managed databases using dump/restore methods or data migration services.

## Next steps

Learn about strategies for [balancing competing priorities](#).

[Balance competing priorities](#)

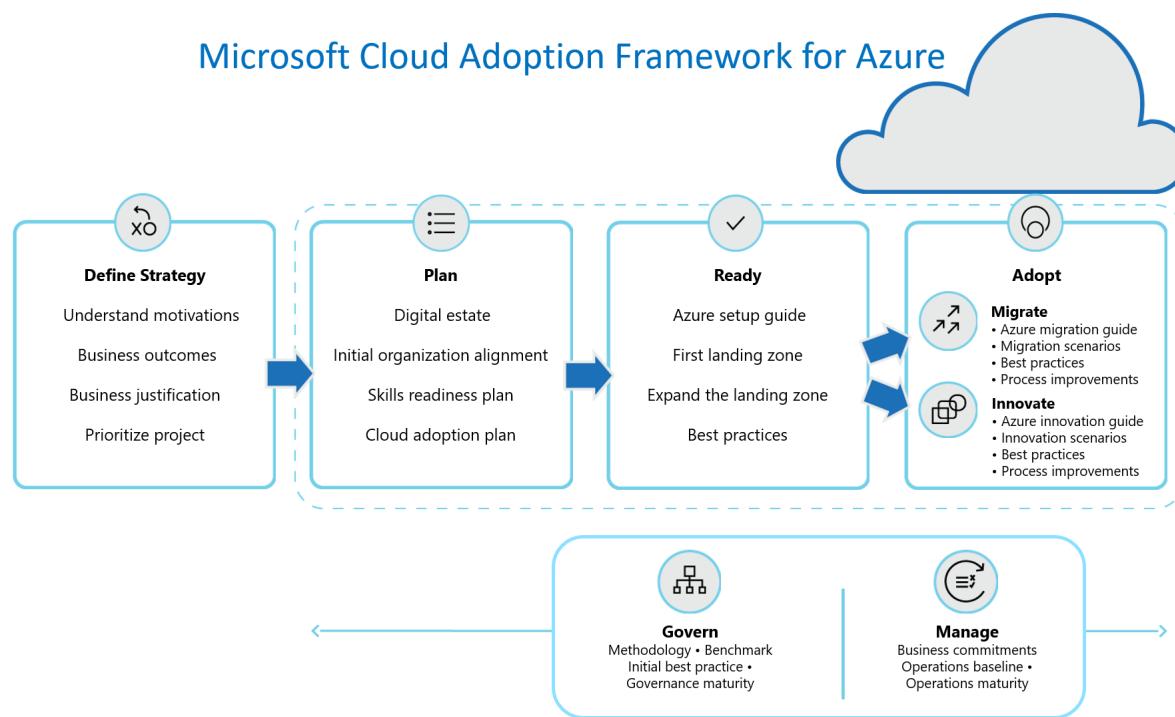
# Balance competing priorities

11/9/2020 • 13 minutes to read • [Edit Online](#)

Embarking on any digital transformation journey acts like a forcing function for stakeholders, across the business and technology teams. The path to success is firmly rooted in the organization's ability to balance competing priorities.

Similar to other digital transformations, cloud adoption will expose competing priorities throughout the adoption lifecycle. Like other forms of transformation, the ability to find balance in those priorities will have a significant impact on the realization of business value. Balancing these competing priorities will require open and sometimes difficult conversations between stakeholders (and sometimes with individual contributors).

This article outlines some of the competing priorities commonly discussed during the execution of each methodology. We hope this advanced awareness will help better prepare for those discussions when developing your cloud adoption strategy.



The following sections align to the flow of the cloud adoption lifecycle visual above. However, it's important to recognize that cloud adoption is iterative (not a sequential process) and these competing priorities will emerge (and sometimes reemerge) at various points along your cloud adoption journey.

## General theme of the Cloud Adoption Framework approach

Monolithic solutions and advanced planning are both built on a series of assumptions that may (or may not) prove to be accurate over time. Adopting the cloud is often a new experience for the business and the technical teams. As with most new experiences or learning opportunities, there is a high probability that those assumptions will be proven false.

Following proven agile principles of delayed technical decisions is the favored approach for most guidance within this framework. That approach follows a consistent pattern: establish a general end-state, move quickly to initial implementation, test and validate assumptions, and refactor early to address assumptions. This type of growth mindset maximizes learning and minimizes risk to business value, but it requires some comfort with ambiguity.

At times, ambiguity can be scarier (or more dangerous) than false assumptions. While this framework leans towards learning and addressing ambiguity during execution, there are many situations that require the team to lean towards analysis-based or assumption-based approaches. The following sections will attempt to illustrate at least one "expanded scope example" in each section to illustrate times when a second deeper iteration would be valuable.

## Balance during the Strategy phase

The core objective of the Strategy methodology is to develop alignment between stakeholders. Once defined, that aligned strategic position will drive behaviors throughout each of the methodologies to ensure that technical decisions align desired business outcomes. Fostering alignment between stakeholders creates a common set competing priorities: **depth of justification** versus **time to business impact**.

**Competing priorities:**

- **Depth of justification:** Stakeholders often want a deep financial analysis and full business justification to be comfortable aligning to a strategic direction. Unfortunately, that level of analysis may require an extended time period to allow for data collection and analysis.
- **Time to business impact:** Conversely, stakeholders are often held accountable for delivering business outcomes within defined time frames. Time consuming analysis and assessment can put those outcomes at risk before the technical work even begins.

**Minimum scope:** Finding this balance requires stakeholder discussions early in the process. The Strategy methodology suggests limiting the scope of alignment during this early effort. In the suggested approach, stakeholders focus on aligning around a set of core motivations, measurable outcomes, and a high-level business justification. Stakeholders should then quickly commit to a small number of initial projects or pilots to drive required learning opportunities.

**Expanded scope example:** If the initial business analysis indicates a high risk of negatively affecting the business, then stakeholders may need to slow down and more cautiously evaluate a deeper analysis during business justification.

## Balance during the Plan phase

Similar to the Strategy phase priorities, during the Plan phase there is a need to balance the depth of initial planning versus delayed technical decisions.

**Competing priorities:**

- **Depth of initial planning** regarding technical implementation in the cloud often contains a high number of assumptions. Especially when the team has skill gaps, the environment suffers from discovery gaps, or the workloads don't have clearly defined architectural end-states. All of these assumptions are common in detailed cloud adoption plans. Experimentation, pilots, and qualitative analysis are required to remove these assumptions.
- **Delayed technical decisions** assume that the later a technical decision can be made, the more accurate that decision will be. Following principles of agile product planning will help delay technical decisions, allowing them to happen at the right time with sufficient information. However, this approach results in a much higher degree of ambiguity in the initial plan.

**Minimum scope:** Agile product development approaches are suggested to drive prompt action within manageable plans. The Plan methodology recommends the following steps to achieve this balance. Inventory the full digital estate using automated discovery tools, but use incremental rationalization to plan as far as the next 1-3 months of work. Ensure proper organizational alignment to move quickly. Create a skills readiness plan for the assigned team. Use the strategy and plan template to quickly deploy an initial backlog.

**Expanded scope example:** At times, delivery of a cloud adoption plan may be responding to a time-sensitive or high-impact business event. When success requires the movement of a high-number of assets in a fixed period of time, the steps above are often followed with a deeper planning effort. The key to success in these scenarios, is to plan enough to get going and then plan for the full engagement. This approach reduces the likelihood of planning blocking business outcomes.

## Balance during the Ready phase

When adoption teams are preparing for their first steps into the cloud, there are often competing priorities between time to adoption and long-term operations. The team may struggle with being well suited to deliver on the task at hand versus being well managed. This struggle is necessary in traditional IT environments, where the act of developing a platform requires physical assets and acquisition cycles. However, when the entire IT platform is defined in code, traditional development tactics (like refactoring) reduce the need to be well managed from the beginning.

### Competing priorities:

- **Long-term operations:** Customers often get blocked by the desire to have a cloud environment that meets feature parity with current operations management, governance, and security systems. In a current study of customers, more than 90% of the customers required support getting past this mindset. This blocker injects months of delay slowing or preventing business impact.
- **Time to adoption:** Cloud-based tools like Azure Policy, Azure Blueprints, and management groups allow for ease of refactoring across the IT platform. Additionally, predefined landing zones provide opinionated positions to accelerate deployment towards an environment that already meets many of the feature parity requirements. Together there are opportunities to accelerate time to market, with minimal impact on long-term operations.

**Minimum scope:** The Ready methodology outlines a direct path from rapid adoption to long-term operations. This approach starts with a basic introduction to the tools that enable environment refactoring. Based on those tools and environmental requirements, customers are guided to a selection of predefined landing zones (each delivered using infrastructure as code models). That code can then be refactored during the course of cloud adoption to improve operations, security, and management postures.

**Expanded scope example:** For teams whose adoption plan calls for a mid-term objective (within 24 months) to host **more than 1,000 assets (apps, infrastructure, or data assets) in the cloud**, a more robust view of landing zones is suggested. In these situations, the Govern and Manage methodologies should be considered during initial landing zone conversations. However, this deeper consideration often adds weeks or months to a cloud adoption plan. To minimize impact on business outcomes, the adoption team should pilot actual workloads in the cloud in parallel to the creation of a more mature landing zone and central architecture solution.

## Balance during the Migrate phase

During migration efforts, it is common for adoption teams to assume that workloads will be rehosted in the cloud in their current as-is configuration. This directly competes with a forward-looking view to rearchitect every workload to better take advantage of cloud capabilities. However, the two are not mutually exclusive and can be complimentary when managed through a common process.

### Competing priorities:

- **Rehost:** Customers often equate migration to a *lift and shift* motion of replicating all assets to the cloud in their current state configuration. This results in little drift within the IT portfolio. This approach is also the fastest way to retire assets in an existing datacenter.
- **Rearchitect:** Modernizing the architecture of each workload maximizes the value of the cloud across cost, performance, and operations. However, this approach is much slower and often requires access to each applications' source code.

**Minimum scope:** During early-stage planning, use the rehost option for planning, with a clear understanding that this option is an initial business assumption and not a technical decision. In the Migrate methodology, the cloud adoption team would then challenge this assumption for each migrated workload. This methodology follows the assess/migrate/promote approach for each workload or group of workloads creating a migration factory. During the Assess phase, the adoption team evaluates technical fit and architecture of each workload. That assessment effort seldom results in a pure lift and shift approach, because many of the components in the architecture tend to be selected for refactoring and modernization.

**Expanded scope example:** For mission-critical or high-sensitivity workloads, like a mainframe or multitier microservices application, a deeper assessment of the workload may be required during the Assess phase. In these rearchitecture situations, customers should use the Microsoft Azure Well-Architected Review and the [Microsoft Azure Well-Architected Framework](#) to refine workload requirements during the assessment.

## Balance during the Innovate phase

True customer-facing innovation creates common conflicting priorities between the need to deliver on a planned feature set and a customer empathy development process.

### Competing priorities:

- **Feature focus:** Initial plans for innovation build on the existing digital estate and cloud capabilities to deliver a set of features that meet a customer need. It's easy to allow the plan to drive technical implementation, leading to a feature focused development effort. This approach often leads to temporary stakeholder satisfaction but reduces the likelihood of driving innovation that impacts customer behaviors.
- **Customer empathy:** Initial plans are an important part of the business side of development and should be included in regular reporting. However, learning, measuring, and building with customer empathy is a more accurate measure of success in an innovation effort. Focusing on the customer over features is more likely to result in both short-term and long-term customer satisfaction and business impact.

**Minimum scope:** The Innovate methodology illustrates how to integrate strategy and plans through business value consensus. The guide then introduces cloud-native tools that can accelerate each discipline of innovation, accompanying best practices for implementation. Finally the process improvements section demonstrates approaches to building customer empathy while respecting plans and strategies across the cloud adoption journey. This approach focuses on delivering innovation with the use of as little technology as is possible.

**Expanded scope example:** At times, an innovation may be dependent on mission-critical or high-sensitivity workloads. When the "customer" is an internal user, the development effort may be both mission-critical and high-sensitivity during the earliest of iterations. For these scenarios, adoption teams should use Microsoft Azure Well-Architected Review and Microsoft Azure Well-Architected Framework to evaluate advanced architectural design early in the process.

## Balance during the Govern phase

The practice of cloud governance is a constant balance between two competing priorities: speed and agility versus a well-governed environment. The cloud governance team focuses on evaluating and minimizing risks to the business through uniform controls and minimizing change. The adoption team focuses on driving business outcomes, which require new risks and inherently creates change.

### Competing priorities:

- **Well-governed:** Every control designed to minimize risk blocks some aspect of change or limits design options. Control is essential to a well-governed environment. However, when controls are designed and deployed in isolation, they can be as damaging as the risks they are intended to prevent.
- **Speed and agility:** Speed and agility are fundamental business requirements in the digital economy. Both require the ability to drive change with minimal blockers to innovation or adoption. When change is driven in

isolation of governance, it generates new risks that could harm the business in unintended ways.

**Minimum scope:** The Govern methodology suggests that neither governance nor adoption should ever happen in isolation. This methodology starts with an understanding of the governance disciplines and a conversation around business risk, policy, and process. As an active member throughout the cloud adoption journey, the governance team can implement a minimum set of guardrails to address the tangible risks within the cloud adoption plan. Over time the governance team can refactor and expand those guardrails to meet new risks. This approach maximizes learning and innovation, while minimizing risk.

**Expanded scope example:** When the business risk is high, especially early in adoption, the cloud governance team may be required to accelerate the expansion of governance implementations. The same guidance and exercises can be used to add this higher level of governance, but timing may have to be accelerated. In some scenarios, an advanced state of governance may even be required during the deployment of the first landing zones.

## Balance during the Manage phase

The IT business model regarding operations management has been continuously evolving over the last decade. As hardware maintenance moves further from IT's core value proposition, the view on operations management has shifted as well. As IT increases a focus on delivering business value, operations management teams are conflicted with balancing no-ops/low-ops versus broad investments.

### Competing priorities:

- **Broad investments:** Investing equally in outage avoidance, rapid recovery, and monitoring across the environment is the traditional approach to operations management. This approach can be costly and sometimes duplicates the supporting products made available by the cloud vendor.
- **No-ops and low-ops:** Use cloud-native operations tools to minimize repetitive and recurring tasks previously delivered by full-time employees. Reducing these operational dependencies in the operations management model frees those employees to drive more value. Alone, this approach can lead to subpar operations support.

**Minimum scope:** The Manage methodology suggests establishing a cloud-native, no-ops baseline.

Acknowledging that the no-ops baseline will not meet all business needs, work with the business to define commitments and better align investments. Expand the baseline to meet common needs for all workloads. Then enable platform teams or specific workload teams to maintain well-managed solutions within a well-managed environment.

**Expanded scope example:** In most environments, a small percentage of workloads whose business value justifies deep investments in operations from IT. In those scenarios, the IT team might want to use Microsoft Azure Well-Architected Review and Microsoft Azure Well-Architected Framework to guide deeper operations.

## Balance during the Organize phase

The competing priorities throughout this article are reflective of IT's drive to deliver on business demands for speed and agility. This same shift is showing up in changes to org charts (or virtual team structures) to empower greater support for business outcomes. As IT leaders reflect on team structures, two competing priorities are commonly addressed: centralized control versus delegated control.

### Competing priorities:

- **Centralized control:** This operating model focuses on centralization of all controls required to enforce rigid policies. In this model, IT serves as a blocker to innovation, speed, and agility. However, IT can ensure a higher degree of stability, compliance, and security.
- **Delegated control:** In this distributed operating model, it is assumed that each DevOps team or business application team will provide their own set of controls, based on the solutions required to deliver on business objectives. In this model, IT provides guardrails to help keep the teams on the road, but minimizes the number

of forced technical constraints whenever possible.

**Minimum scope:** Most organizations will go through a natural set of evolutions over time. The Organize methodology outlines the most common series of evolutions. The suggested guidance is for teams to strive to move towards a cloud center of excellence (CCoE) structure to deliver delegated control approaches.

**Expanded scope example:** There are many situations that would trigger a need for centralized control. Third-party compliance requirements and temporary security exposure are two examples of triggers for centralized control. In these situations, there is commonly a need to establish limiting policies and rigid, fixed controls. However, to enable innovation and adoption to continue, it is encouraged that central IT teams deliver those controls based on criticality and sensitivity of each workload. Providing environments with less control but a reduced scope or risk profile, allows for flexibility even when control is required.

## Next steps

Learn to [balance migration, innovation, and experimentation](#) to maximize the value your cloud migration efforts.

[Balance the portfolio](#)

# Balance the portfolio

11/9/2020 • 9 minutes to read • [Edit Online](#)

Cloud adoption is a portfolio-management effort, cleverly disguised as technical implementation. Like any portfolio management exercise, balancing the portfolio is critical. At a strategic level, this means balancing migration, innovation, and experimentation to get the most out of the cloud. When the cloud adoption effort leans too far in one direction, complexity finds its way into the adoption efforts. This article will guide the reader through approaches to achieve balance in the portfolio.

## General scope expansion

Balancing the portfolio is strategic in nature. As such, the approach taken in this article is equally strategic. To ground the strategy in data-driven decisions, this article assumes the reader has evaluated the existing [digital estate](#) or has begun that process. The objective of this approach is to aid in evaluating workloads to ensure proper balance across the portfolio through qualitative questions and portfolio refinement.

### Document business outcomes

Before balancing the portfolio, it is important to document and share the business outcomes driving the cloud-migration effort. The following table can help document and share desired business outcomes. It's important to note that most businesses are pursuing several outcomes at a time. The importance of this exercise is to clarify the outcomes that are most directly related to the cloud migration effort:

OUTCOME	MEASURED BY	GOAL	TIME FRAME	PRIORITY FOR THIS EFFORT
Reduce IT costs	Datacenter budget	Reduce by \$2M USD	12 months	#1
Datacenter exit	Exit from datacenters	2 datacenters	6 months	#2
Increase business agility	Improve time to market	Reduce deployment time by six months	2 years	#3
Improve customer experience	Customer satisfaction (CSAT)	10% improvement	12 months	#4

### IMPORTANT

The above table is a fictional example and should not be used to set priorities. In many cases, this table could be considered an antipattern by placing cost savings above customer experiences.

The above table could accurately represent the priorities of the cloud strategy team and the cloud adoption team. Due to short-term constraints, this team is placing a higher emphasis on IT cost reduction and prioritizing a datacenter exit as a means to achieve the desired IT cost reductions. However, by documenting the competing priorities in this table, the cloud adoption team is empowered to help the cloud strategy team identify opportunities to better align implementation of the overarching portfolio strategy.

### Move fast while maintaining balance

The guidance regarding [incremental rationalization of the digital estate](#) suggests an approach in which the rationalization starts with an unbalanced position. The cloud strategy team should evaluate every workload for compatibility with a rehost approach. Such an approach is suggested because it allows for the rapid evaluation of

a complex digital estate based on quantitative data. Making such an initial assumption allows the cloud adoption team to engage quickly, reducing time to business outcomes. However, as stated in that article, qualitative questions will provide the necessary balance in the portfolio. This article documents the process for creating the promised balance.

### Importance of sunset and retire decisions

The table in the [documenting business outcomes](#) section above misses a key outcome that would support the number one objective of reducing IT costs. When IT costs reductions rank anywhere in the list of business outcomes, it is important to consider the potential to sunset or retire workloads. In some scenarios, cost savings can come from not migrating workloads that don't warrant a short-term investment. Some customers have reported cost savings in excess of 20% total cost reductions by retiring underutilized workloads.

To balance the portfolio, better reflecting sunset and retire decisions, the cloud strategy team and the cloud adoption team are encouraged to ask the following questions of each workload within assess and migrate phases:

- Has the workload been used by end users in the past six months?
- Is end-user traffic consistent or growing?
- Will this workload be required by the business 12 months from now?

If the answer to any of these questions is "no", then the workload could be a candidate for retirement. If retirement potential is confirmed with the app owner, then it may not make sense to migrate the workload. This prompts for a few qualification questions:

- Can a retirement plan or sunset plan be established for this workload?
- Can this workload be retired prior to the datacenter exit?

If the answer to both of these questions is "yes", then it would be wise to consider *not* migrating the workload. This approach would help meet the objectives of reducing costs and exiting the datacenter.

If the answer to either question is "no", it may be wise to establish a plan for hosting the workload until it can be retired. This plan could include moving the assets to a lower-cost datacenter or alternative datacenter, which would also accomplish the objectives of reducing costs and exiting one datacenter.

## Adopt process changes

Balancing the portfolio requires additional qualitative analysis during the Adopt phase, which will help drive simple portfolio rationalization.

Based on the data from the table in the [documenting business outcomes](#) section above, there is a likely risk of the portfolio leaning too far into a migration-focused execution model. If customer experience was top priority, an innovation heavy portfolio would be more likely. Neither is right or wrong, but leaning too far in one direction commonly results in diminishing returns, adds unnecessary complexity, and increases execution time related to cloud adoption efforts.

To reduce complexity, you should follow a traditional approach to portfolio rationalization, but in an iterative model. The following steps outline a qualitative model to such an approach:

- The cloud strategy team maintains a prioritized backlog of workloads to be migrated.
- The cloud strategy team and the cloud adoption team host a release planning meeting prior to the completion of each release.
- In the release planning meeting, the teams agree on the top 5 to 10 workloads in the prioritized backlog.
- Outside of the release planning meeting, the cloud adoption team asks the following questions of application owners and subject matter experts:
  - Could this application be replaced with a platform as a service (PaaS) equivalent?
  - Is this application a third-party application?

- Has budget been approved to invest in ongoing development of the application in the next 12 months?
- Would additional development of this application improve the customer experience? Create a competitive differentiator? Drive additional revenue for the business?
- Will the data within this workload contribute to a downstream innovation related to BI, machine learning, IoT, or related technologies?
- Is the workload compatible with modern application platforms like Azure App Service?
- The answers to the above questions and any other required qualitative analysis would then influence adjustments to the prioritized backlog. These adjustments may include:
  - If a workload could be replaced with a PaaS solution, it may be removed from the migration backlog entirely. At a minimum, additional due diligence to decide between rehost and replace would be added as a task, temporarily reducing that workload's priority from the migration backlog.
  - If a workload is (or should be) undergoing development advancement, then it may best fit into a refactor-rearchitect-rebuild model. Since innovation and migration require different technical skills, applications that align to a refactor-rearchitect-rebuild approach should be managed through an innovation backlog rather than a migration backlog.
  - If a workload is part of a downstream innovation, then it may make sense to refactor the data platform, but leave the application layers as a rehost candidate. Minor refactoring of a workload's data platform can often be addressed in a migration or an innovation backlog. This rationalization outcome may result in more detailed work items in the backlog, but otherwise no change to priorities.
  - If a workload isn't strategic but is compatible with modern, cloud-based application hosting platforms, then it may be wise to perform minor refactoring on the application to deploy it as a modern app. This can contribute to the overall savings by reducing the overall IaaS and OS licensing requirements of the cloud migration.
  - If a workload is a third-party application and that workload's data isn't planned for use in a downstream innovation, then it may be best to leave as a rehost option on the backlog.

These questions shouldn't be the extent of the qualitative analysis completed for each workload, but they help guide a conversation about addressing the complexity of an imbalanced portfolio.

## Migration process changes

During migration, portfolio balancing activities can have a negative impact on migration velocity (the speed at which assets are migrated). The following guidance will expand on why and how to align work to avoid interruptions to the migration effort.

Portfolio rationalization requires diversity of technical effort. It is tempting for cloud adoption teams to match that portfolio diversity within migration efforts. Business stakeholders often ask for a single cloud adoption team to address the entire migration backlog. This is seldom an advisable approach, in many cases this can be counterproductive.

These diverse efforts should be segmented across two or more cloud adoption teams. Using a two-team model as an example mode of execution, team 1 is the migration team and team 2 is the innovation team. For larger efforts, these teams could be further segmented to address other approaches like replace/PaaS efforts or minor refactoring. The following outlines the skills and roles needed to rehost, refactor, or minor refactoring:

**Rehost:** Rehost requires team members to implement infrastructure focused changes. Generally using a tool like Azure Site Recovery to migrate VMs or other assets to Azure. This work aligns well to datacenter admins or IT implementors. The cloud migration team is well structured to deliver this work at high scale. This is the fastest approach to migrate existing assets in most scenarios.

**Refactor:** Refactor requires team members to modify source code, change the architecture of an application, or adopt new cloud services. Generally this effort would use development tools like Visual Studio and deployment pipeline tools like Azure DevOps to redeploy modernized applications to Azure. This work aligns well to

application development roles or DevOps pipeline development roles. The cloud innovation team is best structured to deliver this work. It can take longer to replace existing assets with cloud assets in this approach, but the apps can take advantage of cloud-native features.

**Minor refactoring:** Some applications can be modernized with minor refactoring at the data or application level. This work requires team members to deploy data to cloud-based data platforms or to make minor configuration changes to the application. This may require limited support for data or application development subject matter experts. However, this work is similar to the work conducted by IT implementors when deploying third-party apps. This work could easily align with the cloud migration team or the cloud strategy team. While this effort is not nearly as fast as a rehost migration, it takes less time to execute than refactor efforts.

During migration, efforts should be segmented in the three ways listed above and executed by the appropriate team in the appropriate iteration. While you should diversify the portfolio, also ensure that efforts stay very focused and segregated.

## Next steps

Understand how [global market decisions](#) can affect your transformation journey.

[Understand global markets](#)

# How will global market decisions affect the transformation journey?

11/9/2020 • 2 minutes to read • [Edit Online](#)

The cloud opens new opportunities to perform on a global scale. Barriers to global operations are significantly reduced, by empowering companies to deploy assets in market, without the need to invest heavily in new datacenters. Unfortunately, this also adds a great deal of complexity from technical and legal perspectives.

## Data sovereignty

Many geopolitical regions have established data sovereignty regulations. Those regulations restrict where data can be stored, what data can leave the country of origin, and what data can be collected about citizens of that region. Before operating any cloud-based solution in a foreign geography, you should understand how that cloud provider handles data sovereignty. For more information about Azure's approach for each geography, see [Azure geographies](#). For more information about compliance in Azure, see [Privacy at Microsoft](#) in the Microsoft Trust Center.

The remainder of this article assumes legal counsel has reviewed and approved operations in a foreign country.

## Business units

It is important to understand which business units operate in foreign countries, and which countries are affected. This information will be used to design solutions for hosting, billing, and deployments to the cloud provider.

## Employee usage patterns

It is important to understand how global users access applications that are not hosted in the same country as the user. Global wide-area networks (WANs) route users based on existing networking agreements. In a traditional on-premises world, some constraints limit WAN design. Those constraints can lead to poor user experiences if not properly understood before cloud adoption.

In a cloud model, commodity internet opens up many new options as well. Communicating the spread of employees across multiple geographies can help the cloud adoption team design WAN solutions that create positive user experiences and potential reduce networking costs.

## External user usage patterns

It is equally important to understand the usage patterns of external users, like customers or partners. Much like employee usage patterns, external user usage patterns can negatively affect performance of cloud deployments. When a large or mission-critical user base resides in a foreign country, it could be wise to include a global deployment strategy into the overall solution design.

## Next steps

Learn about the [skills needed during the Strategy phase](#) of your cloud adoption journey.

[Skills needed during the Strategy phase](#)

# Define a security strategy

11/9/2020 • 23 minutes to read • [Edit Online](#)

The ultimate objectives for a security organization don't change with adoption of cloud services, but how those objectives are achieved will change. Security teams must still focus on reducing business risk from attacks and work to get confidentiality, integrity, and availability assurances built into all information systems and data.

## Modernize your security strategy

Security teams need to modernize strategies, architectures, and technology as the organization adopts cloud and operates it over time. While the size and number of changes can initially seem daunting, the modernization of the security program allows security to shed some painful burdens associated with legacy approaches. An organization may temporarily operate with legacy strategy and tooling, but this approach is difficult to sustain with the pace of change in cloud and the threat environment:

- Security teams are likely to be left out of cloud adoption decision making if they take a legacy mindset of "arms-length" security where the answer always starts with "no" (instead of working together with IT and business teams to reduce risk while enabling the business).
- Security teams will have a difficult time detecting and defending against cloud attacks if they use only legacy on-premises tooling and exclusively adhere to network perimeter only doctrine for all defenses and monitoring. Defending at cloud scale mandates the use of cloud native detection and automation capabilities and the introduction of an identity perimeter to help monitor and protect cloud and mobile assets.

Because this transformation can be significant, we recommend security teams take an agile approach to modernizing security that rapidly modernizes the most critical aspects of the strategy and then continuously improving incrementally after that.

### Security of the cloud and from the cloud

As your organization adopts cloud services, security teams will be working towards two main objectives:

- **Security \*of\* the cloud (securing cloud resources):** Security should be integrated into the planning and operation of cloud services to ensure that those core security assurances are consistently applied across all resources.
- **Security \*from\* the cloud (using the cloud to transform security):** Security should immediately start planning and thinking about how to use cloud technologies to modernize security tools and processes, particularly natively integrated security tools. More and more security tools are being hosted in the cloud and providing capabilities that are difficult or impossible to do in an on-premises environment.

Many organizations start by treating cloud resources as an additional *virtual datacenter*, which works very well as a starting point for security of the cloud. As organizations modernize using security from the cloud, most will find themselves quickly outgrowing this model of thinking. Securing a software-defined datacenter using cloud-hosted tools enables capabilities beyond what on-premises models can offer:

- Rapid enablement and scaling of security capabilities.
- Highly effective asset inventory and security configuration hygiene discovery.
- Continuous assessment of the organization's security posture and controls.
- Vastly improved threat detection that uses vast repositories of threat intelligence and virtually unlimited processing/storage of the cloud.

### The right level of security friction

Security naturally creates friction that slows down processes, it is critical to identifying which elements are healthy

in your DevOps and IT processes and which are not:

- **Healthy friction:** Much like the resistance in exercise makes a muscle stronger, integrating the right level of security friction strengthens the system or app by forcing critical thinking at the right time. This typically takes the form of considering how and why an attacker may try to compromise an application or system during design, and reviewing, identifying, and ideally fixing potential vulnerabilities an attacker can exploit in software code, configurations, or operational practices.
- **Unhealthy friction:** Impedes more value than it protects. This often happens when security bugs generated by tools have a high false positive rate (such as false alarms) or when the effort to discover or fix security issues far exceeds the potential impact of an attack.

### Standalone and integrated responsibilities

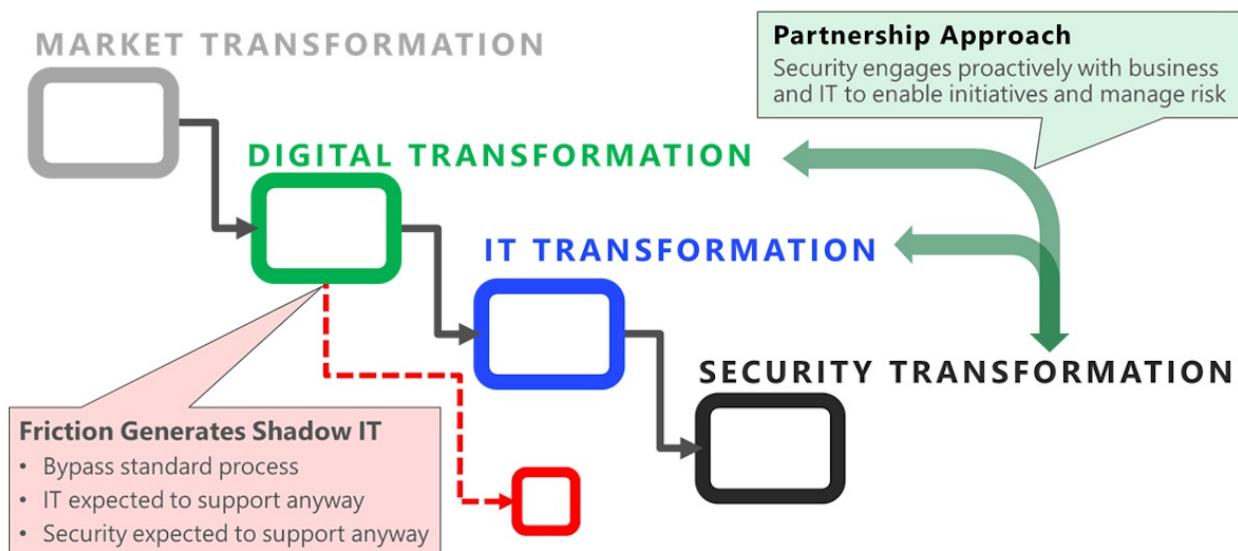
Providing confidentiality, integrity, and availability assurances requires security experts to operate dedicated security functions as well as work closely with other teams in the organization:

- **Unique security functions:** Security teams perform independent functions that are not found elsewhere in the organization, such as security operations, vulnerability management, and other functions.
- **Integrating security into other functions:** Security teams also serve as subject matter experts to other teams and functions in the organization who are driving business initiatives, assessing risk, designing or developing applications, and operating IT systems. Security teams advise these teams with expertise and context on attackers, attack methods and trends, vulnerabilities that could allow unauthorized access, and options for mitigation steps or workarounds and their potential benefits or pitfalls. This function of security resembles that of a quality function as it will be woven into many places large and small in support of a single outcome.

Executing on these responsibilities whilst keeping up with the rapid pace of change in the cloud and the transformation of business will require security teams to modernize their tools, technologies and processes.

## Transformations, mindsets, and expectations

Many organizations are managing a chain of multiple simultaneous transformations in the organization. These internal transformations typically start because nearly all external markets are transforming to meet new customer preferences for mobile and cloud technologies. Organizations often face the competitive threat of new startups and the digital transformation of traditional competitors who can disrupt the market.



The internal transformation process typically includes:

- **Digital transformation** of the business to capture new opportunities and stay competitive against digital native startups.

- **Technology transformation** of the IT organization to support the initiative with cloud services, modernized development practices, and related changes.
- **Security transformation** to both adapt to the cloud and simultaneously address an increasingly sophisticated threat environment.

### **Internal conflict can be costly**

Change creates stress and conflict, which can grind decision making to a halt. This is particularly true in security where accountability for security risk is often misplaced on the subject matter experts (security teams), rather than on the owners of the assets (business owners) that are accountable for business outcomes and all other risk types. This misplaced accountability often happens because all stakeholders incorrectly view security as a technical or absolute problem to be solved, rather than a dynamic ongoing risk like corporate espionage and other traditional criminal activities.

During this time of transformation, leadership of all teams must work actively to reduce conflict that can both derail critical projects and incentivize teams to bypass security risk mitigation. Internecine conflict between teams can result in:

- **Increased security risk** such as avoidable security incidents or increased business damage from attacks (particularly when teams get frustrated by security and bypass normal processes or when outdated security approaches are easily bypassed by attackers).
- **Negative impact on the business or mission** such as when business processes aren't enabled or updated fast enough to meet market needs (often when security processes hold up key business initiatives).

It's critical to stay aware of relationship health within and between teams to help them navigate the shifting landscape that could leave valuable team members insecure and unsettled. Patience, empathy, and education on these mindsets and the positive potential of the future will help your teams better navigate this period, driving good security outcomes for the organization.

Leaders can help drive culture changes with concrete proactive steps like:

- Publicly modeling the behavior they expect of their teams.
- Being transparent about the challenges of the changes, including highlighting their own struggles to adapt.
- Regularly reminding teams of the urgency and importance of modernizing and integrating security.

### **Cybersecurity resilience**

Many classic security strategies have been focused solely on preventing attacks, which is not sufficient for modern threats. Security teams must ensure their strategy goes beyond this and also enables rapid attack detection, response, and recovery to increase resilience. Organizations must assume that attackers will compromise some resources (sometimes called "assume breach") and work to ensure that resources and technical designs are balanced between attack prevention and attack management (rather than the typical default approach of only attempting to prevent attacks).

Many organizations are already on this journey because they have been managing the steady rise in volume and sophistication of attacks in recent years. This journey often starts with the first major incident, which can be an emotional event where people lose their prior sense of invulnerability and safety. While not as severe as a loss of life, this event can trigger similar emotions starting with denial and ultimately ending in acceptance. This assumption of "failure" may be difficult for some to accept at first, but it has strong parallels to the well-established "fail-safe" engineering principle and the assumption allows your teams to focus on a better definition of success: resilience.

The functions of the [NIST cybersecurity framework](#) serve as a useful guide on how to balance investments between the complementary activities of identify, protect, detect, respond, and recover in a resilient strategy.

More on cybersecurity resilience and the ultimate goals of cybersecurity controls is discussed in [How do you keep your organization's risk down](#).

## How the cloud is changing security

Shifting to the cloud for security is more than a simple technology change, it is a generational shift in technology akin to moving from mainframes to desktops and onto enterprise servers. Successfully navigating this change requires fundamental shifts in expectations and mindset by security teams. Adopting the right mindsets and expectations will reduce conflict within your organization and increase the effectiveness of security teams.

While these could be part of any security modernization plan, the rapid pace of change in the cloud makes adopting them an urgent priority.

- **Partnership with shared goals.** In this age of fast paced decisions and constant process evolution, security can no longer adopt an "arms-length" approach to approving or denying changes to the environment. Security teams must partner closely with business and IT teams to establish shared goals around productivity, reliability, and security and work collectively with those partners to achieve them.

This partnership is the ultimate form of "shift left"—the principle of integrating security earlier in the processes to make fixing security issues easier and more effective. This requires a culture change by all involved (security, business, and IT), requiring each to learn the culture and norms of other groups while simultaneously teaching others about their own.

Security teams must:

- **Learn** the business and IT objectives and why each is important and how they are thinking about achieving them as they transform.
- **Share** why security is important in the context of those business goals and risks, what other teams can do to meet security goals, and how they should do it.

While not an easy task, it is essential for sustainably securing the organization and its assets. This partnership will likely result in healthy compromises where only the minimum security, business, and reliability goals may be met initially, but incrementally improve steadily over time.

- **Security is an ongoing risk, not a problem.** You can't "solve" crime. At its core, security is just a risk management discipline, which happens to be focused on malicious actions by humans rather than natural events. Like all risks, security is not a problem that can be fixed by a solution, it is a combination of the likelihood and impact of damage from a negative event, an attack. It is most comparable to traditional corporate espionage and criminal activities where organizations face motivated human attackers who have financial incentive to successfully attack the organization.
- **Success in either productivity or security requires both.** An organization must focus on both security and productivity in today's "innovation or become irrelevant" environment. If the organization is not productive and driving new innovation, it may lose competitiveness in the marketplace that causes it to weaken financially or eventually fail. If the organization is not secure and loses control of assets to attackers, it may lose competitiveness in the marketplace that causes it to weaken financially and eventually fail.
- **Nobody's perfect.** No organization is perfect at adopting the cloud, not even Microsoft. Microsoft's IT and security teams grapple with many of the same challenges that our customers do such as figuring out how to structure programs well, balancing supporting legacy software with supporting cutting edge innovation, and even technology gaps in cloud services. As these teams learn how to better operate and secure the cloud, they are actively sharing their lessons learned via documents like this along with others on the [IT showcase site](#), while continuously providing feedback to our engineering teams and third-party vendors to improve their offerings.

Based on our experience, we recommend that teams are held to a standard of continuous learning and improvement rather than a standard of perfection.

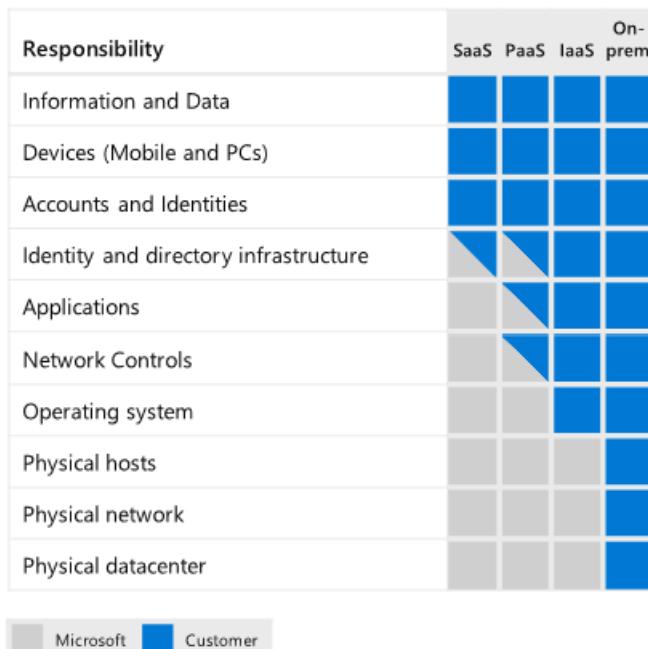
- **Opportunity in transformation.** It's important to view digital transformation as a positive opportunity for security. While it's easy to see the potential downsides and risk of this change, it's easy to miss the massive opportunity to reinvent the role of security and earn a seat at the table where decisions are made.

Partnering with the business can result in increased security funding, reduce wasteful repetitive efforts in security, and make working in security more enjoyable as they will be more connected to the organization's mission.

## Adopting the shared responsibility model

Hosting IT services in the cloud splits the operational and security responsibilities for workloads between the cloud provider and the customer tenant, creating a de facto partnership with shared responsibilities. All security teams must study and understand this shared responsibility model to adapt their processes, tools, and skill sets to the new world. This will help avoid inadvertently creating gaps or overlaps in your security posture resulting in security risks or wasted resources.

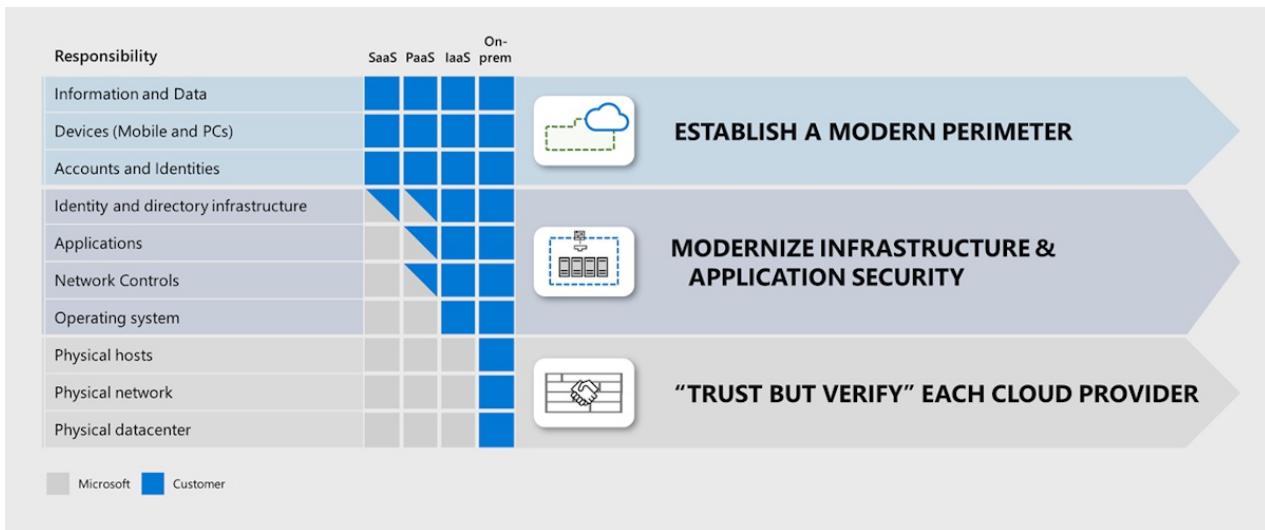
This diagram illustrates how security responsibilities will be distributed between cloud vendors and cloud customer organizations in a de facto partnership:



As there are different models of cloud services, the responsibilities for each workload will vary depending on whether it is hosted on software as a service (SaaS), platform as a service (PaaS), infrastructure as a service (IaaS), or in an on-premises datacenter.

## Building security initiatives

This diagram illustrates the three primary security initiatives that most security programs should follow to adjust their security strategy and security program goals for the cloud:



Building a resilient security posture in the cloud requires several parallel complementary approaches:

- **Trust but verify:** For responsibilities performed by the cloud provider, organizations should take a "trust but verify" approach. Organizations should evaluate the security practices of their cloud providers and the security controls they offer to ensure the cloud provider meets the security needs of the organization.
- **Modernize infrastructure and application security:** For technical elements under the organization's control, prioritize modernizing security tooling and associated skill sets to minimize coverage gaps for securing resources in the cloud. This is composed of two different complementary efforts:
  - **Infrastructure security:** Organizations should use the cloud to modernize their approach to protecting and monitoring the common components used by many applications, such as operating systems, networks, and container infrastructure. These cloud capabilities can often include managing infrastructure components across both IaaS and on-premises environments. Optimizing this strategy is important because this infrastructure is a dependency of the applications and data that run on it, which often enable critical business processes and store critical business data.
  - **Application security:** Organizations should also modernize the way they secure the unique applications and technology that is developed by or for their organization. This discipline is changing rapidly with the adoption of agile DevOps processes, the increasing use of open source components, and introduction of cloud APIs and cloud services to replace application components or interconnect applications.

Getting this right is critical because these applications often enable critical business processes and store critical business data.

- **Modern perimeter:** Organizations should have a comprehensive approach for protecting data across all workloads, organizations should establish a modern perimeter of consistent, centrally managed identity controls to protect their data, devices, and accounts. This is heavily influenced by a zero trust strategy discussed in detail in [Module 3 of the CISO workshop](#).

## Security and trust

Note that the use of the word *trust* in security can be confusing. This documentation refers to it in two ways that illustrate useful applications of this concept:

- **Zero trust** is a common industry term for a strategic approach to security that assumes a corporate or intranet network is hostile (worthy of "zero trust") and designs security accordingly.
- **Trust but verify** is an expression that captures the essence of two different organizations working together toward a common goal despite having some other potentially divergent interests. This concisely captures many of the nuances of the early stages of partnering with a commercial cloud provider for organizations.

A cloud provider and their practices and processes can be accountable to meet contractual and regulatory

requirements and could earn or lose trust. A network is a nonliving connection which cannot face consequences if it is used by attackers (much like you cannot hold a road or a car accountable for criminals using them).

## How cloud is changing security relationships and responsibilities

As with previous transitions to a new generation of technology like desktop computing and enterprise server computing, the shift to cloud computing is disrupting long-established relationships, roles, responsibilities, and skill sets. The job descriptions we have become accustomed to over the last few decades do not cleanly map to an enterprise that now includes cloud capabilities. As the industry collectively works to normalize a new model, organizations will have to focus on providing as much clarity as possible to help manage the uncertainty of ambiguity during this period of change.

Security teams are affected by these changes in the business and technology they support as well as their own internal modernization efforts to better orient to threat actors. Attackers are actively evolving to constantly search for the easiest weak points to exploit in the people, process, and technology of the organization and security must develop capabilities and skills to address these angles.

This section describes the key relationships that frequently change on the journey to the cloud, including lessons learned on minimizing risk and embracing the opportunities to improve:

- **Between security and business stakeholders:** Security leadership will need to increasingly partner with business leaders to enable organizations to reduce risk. Security leaders should support business decision making as security subject matter expert (SMEs) and should strive to grow into trusted advisors to these business leaders. This relationship will help ensure business leaders consider security risks while making business decisions, inform security of business priorities, and help ensure security investments are prioritized appropriately alongside other investments.
- **Between security leadership and team members:** Security leadership should take these insights from business leadership back to their teams to guide their investment priorities.

By setting a tone of cooperation with business leaders and their teams rather than a classic 'arms length' relationship, security leaders can avoid an adversarial dynamic that impedes both security and productivity goals.

Security leaders should strive to provide clarity to their team on how to manage their daily decisions on productivity and security tradeoffs as this may be new to many on their teams.

- **Between application and infrastructure teams (and cloud providers):** This relationship is undergoing significant changes because of multiple trends in the IT and security industry aimed at increasing innovation speed and developer productivity.

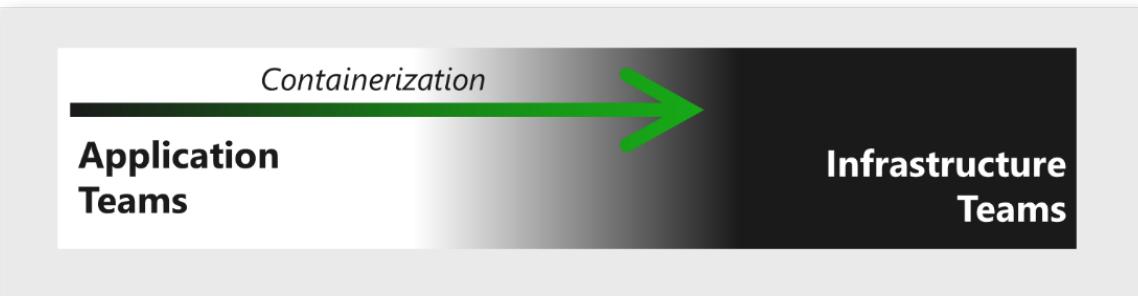
The old norms and organizational functions have been disrupted, but new norms and functions are still emerging, so we recommend accepting the ambiguity, keeping up with current thinking, and experiment with what works for your organizations until it does. We don't recommend adopting a wait-and-see approach in this space because it might put your organization at a major competitive disadvantage.

These trends are challenging the traditional norms for roles and relationships of applications and infrastructure:

- **DevOps-fusing disciplines:** In its ideal state, this effectively creates a single highly functional team that combines both sets of subject matter expertise together to rapidly innovate, release updates, and resolve issues (security and otherwise). While this ideal state will take some time to achieve and the responsibilities in the middle are still very ambiguous, organizations are already reaping some benefits of rapid releases because of this cooperative approach. Microsoft recommends integrating security into this cycle to help learn those cultures, share security learnings, and work towards a common goal of rapidly releasing secure and reliable applications.



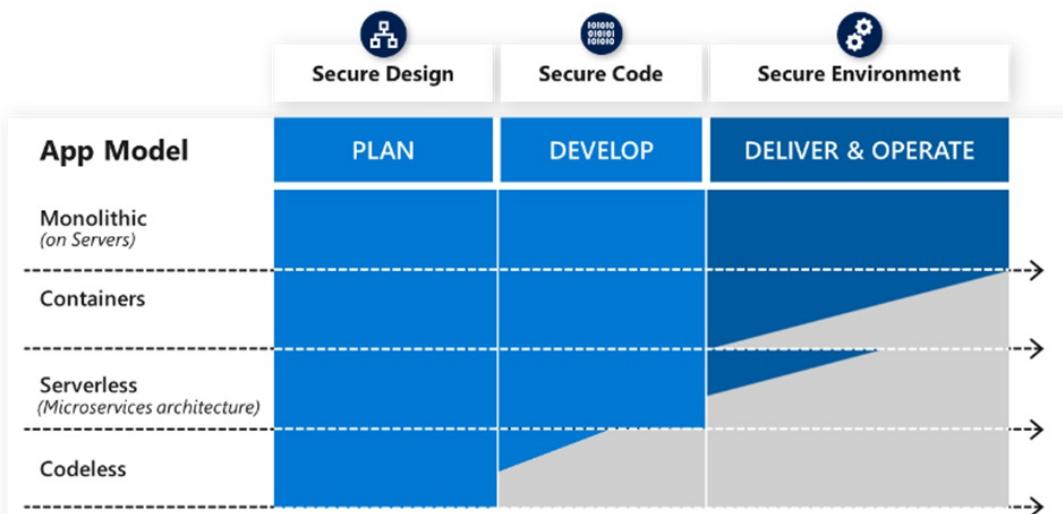
- Containerization becoming a common infrastructure component: Applications are increasingly being hosted and orchestrated by technologies like Docker, Kubernetes, and similar technologies. These technologies simplify development and release by abstracting many elements of the setup and configuration of the underlying operating system.



While containers began as an application development technology managed by development teams, it is becoming a common infrastructure component that is increasingly shifting to infrastructure teams. This transition is still in progress at many organizations, but it is a natural and positive direction many of the current challenges will be best solved with traditional infrastructure skill sets like networking, storage, and capacity management.

Infrastructure teams and security team members that support them should be provided with training, processes, and tooling to help manage, monitor, and secure this technology.

- Serverless and cloud application services: One of the dominant trends in industry right now is reducing the amount of time and development work required to build or update applications.



Developers are also increasingly using cloud services to:

- Run code instead of hosting apps on virtual machines (VMs) and servers.
- Provide application functions instead of developing their own components. This has led to a

*serverless* model that uses existing cloud services for common functions. The number and variety of cloud services (and their pace of innovation) has also exceeded the ability of security teams to evaluate and approve the use of those services, leaving them to choose between allowing developers to use any service, attempting to prevent the development teams from using unapproved services, or trying to find a better way.

- **Codeless apps and Power Apps:** Another emerging trend is the use of codeless technologies like Microsoft Power Apps. This technology enables people without coding skills to create applications that achieve business outcomes. Because of this low friction and high value potential, this trend has the potential to rise in popularity quickly and security professionals would be wise to rapidly understand its implications. Security efforts should be focused on the areas where a human could make a mistake in the application, namely the design of the application and asset permissions via threat modeling the application components, interactions/relationships, and role permissions.
- **Between developers and open source component authors:** Developers are also increasing efficiency by using open source components and libraries instead of developing their own components. This brings value through efficiency, but also introduces security risks by creating an external dependency and a requirement to properly maintain and patch those components. Developers are effectively assuming the risk of security and other bugs when they use these components and have to ensure there is a plan to mitigate them at the same standards as code they would develop.
- **Between applications and data:** The line between security of data and applications is becoming blurred in places and new regulations are creating a need for closer cooperation between data/privacy teams and security teams:
  - **Machine learning (machine learning) algorithms:** machine learning algorithms are similar to applications in that they are designed to process data to create an outcome. The key differences are:
    - **High-value machine learning:** Machine learning often confers a significant competitive advantage and is often considered sensitive intellectual property and a trade secret.
    - **Sensitivity imprint:** Supervised machine learning is tuned using data sets, which imprints characteristics of the dataset on the algorithm. Because of this, the tuned algorithm may be considered sensitive because of the dataset used to train it. For example, training a machine learning algorithm to find secret army bases on a map using a dataset of secret army bases would make it a sensitive asset.

#### NOTE

Not all examples are obvious, so it's critical to bring a team together with the right stakeholders from data science teams, business stakeholders, security teams, privacy teams, and others. These teams should have a responsibility to meet common goals of innovation and responsibility. They should address common issues such as how and where to store copies of data in insecure configurations, how to classify algorithms, as well as any concerns of your organizations.

Microsoft has published our [principles of responsible AI](#) to guide our own teams and our customers.

- **Data ownership and privacy:** Regulations like GDPR have increased the visibility of data issues and applications. Application teams now have the ability to control, protect, and track sensitive data at a level comparable to tracking financial data by banks and financial institutions. Data owners and applications teams need to build a rich understanding of what data applications store and what controls are required.
- **Between organizations and cloud providers:** As organizations host workloads in the cloud, they are entering into a business relationship with each of those cloud providers. The use of cloud services often brings business value such as:

- **Accelerating digital transformation initiatives** by reducing time to market for new capabilities.
- **Increasing value of IT and security activities** by freeing teams to focus on higher value (business-aligned) activities rather than lower-level commodity tasks that are provided more efficiently by cloud services on their behalf.
- **Increased reliability and responsiveness:** Most modern clouds also have extremely high uptime compared to traditional on-premises datacenters and have shown they can scale rapidly (such as during the COVID-19 pandemic) and provide resiliency following natural events like lightning strikes (which would have kept many on-premises equivalents down for much longer).

While extremely beneficial, this shift to the cloud is not without risk. As organizations adopt cloud services, they should consider potential risk areas including:

- **Business continuity and disaster recovery:** Is the cloud provider financially healthy with a business model that's likely to survive and thrive during your organization's use of the service? Has the cloud provider made provisions to allow customer continuity if the provider experiences financial or other failure, such as providing their source code to customers or open-sourcing it?

For more information and documents regarding Microsoft's financial health, see [Microsoft investor relations](#).

- **Security:** Does the cloud provider follow industry best practices for security? Has this been validated by independent regulatory bodies?
  - [Microsoft Cloud App Security](#) allows you to discover usage of over 16,000 cloud apps, which are ranked and scored based on more than 70 risk factors to provide you with ongoing visibility into cloud use, shadow IT, and the risk that shadow IT poses to your organization.
  - The [Microsoft Service Trust Portal](#) makes regulatory compliance certifications, audit reports, pen tests, and more available to customers. These documents include many details of internal security practices (notably the SOC 2 type 2 report and FedRAMP Moderate system security plan).
- **Business competitor:** Is the cloud provider a significant business competitor in your industry? Do you have sufficient protections in the cloud services contract or other means to protect your business against potentially hostile actions?

Review [this article](#) for commentary on how Microsoft avoids competing with cloud customers.

- **Multicloud:** Many organizations have a de facto or intentional multicloud strategy. This could be an intentional objective to reduce reliance on a single supplier or to access unique best of breed capabilities, but can also happen because developers chose preferred or familiar cloud services, or your organization acquired another business. Regardless of the reason, this strategy can introduce potential risks and costs that have to be managed including:
  - **Downtime from multiple dependencies:** Systems architected to rely on multiple clouds are exposed to more sources of downtime risk as disruptions in the cloud providers (or your team's use of them) could cause an outage/disruption of your business. This increased system complexity would also increase the likelihood of disruption events as team members are less likely to fully understand a more complex system.
  - **Negotiating power:** Larger organizations also should consider whether a single-cloud (mutual commitment/partnership) or multicloud strategy (ability to shift business) will achieve greater influence over their cloud providers to get their organization's feature requests prioritized.
  - **Increased maintenance overhead:** IT and security resources already are overburdened from their existing workloads and keeping up with the changes of a single cloud platform. Each additional platform further increases this overhead and takes team members away from higher value activities like streamlining technical process to speed business innovation, consulting with business groups on more effective use of technologies, and so on.

- **Staffing and training:** Organizations often do not consider the staffing requirements necessary to support multiple platforms and the training required to maintain knowledge and currency of new features which are released in a rapid pace.

# Cloud monitoring guide: Formulate a monitoring strategy

11/9/2020 • 20 minutes to read • [Edit Online](#)

As you undergo your digital transformation to the cloud, it's important that you plan and develop an effective cloud monitoring strategy with participation of developers, operations staff, and infrastructure engineers. The strategy should be growth-oriented, defined minimally, then refined iteratively; always aligned with business needs. Its outcome delivers an agile operations modality centered around the ability of the organization to proactively monitor complex distributed applications the business depends on.

## Where to start?

To ease your journey to the cloud, use the [Strategy phase](#) and the [Plan phase](#) of the Cloud Adoption Framework. Monitoring influences and justifies the motivations, business outcomes, and initiatives. Include monitoring in the strategy and plan phases, your initiatives, and projects. For example, examine how the first adoption project establishes early operations management in Azure. Imagine what the cloud operating model needs to look like, including the role of monitoring. Monitoring is best served with a service-based approach, as an operations function, where monitoring is an advisory service and a provider of expertise to business and IT consumers.

The following are important areas that strongly influence a sound monitoring strategy:

- Monitor the health of your applications, based on its components and their relationship with other dependencies. Start with the cloud service platform, resources, the network, and lastly the application by collecting metrics and logs where applicable. For the hybrid cloud model, include on-premises infrastructure and other systems the application relies on.
- Include measuring the end user's experience in your applications performance monitoring plan by mimicking your customer's typical interactions with the application.
- Ensure security requirements correspond with your organizations security compliance policy.
- Align alerts with what is considered a relevant and practical incident (such as warnings and exceptions) and align severity with its significance following your incident priority and urgency escalation matrix.
- Collect only the metrics and logs that are useful, measurable, and identifiable to the business and IT organization.
- Define an integration plan with existing ITSM solutions such as remedy or ServiceNow for incident generation or upstream monitoring. Determine which alerts should be forwarded, whether alert enrichment is required to support specific filtering requirements, and how to configure.
- Understand who needs visibility, what they need to see, and how it should be visualized based on their roles and responsibilities.

At the heart of operations management, your IT organization needs to establish centralized governance and strict delegation over approaches to build, operate, and manage IT services.

### Initial strategy goals

As an architect or strategic planner, you may need to formulate an early strategy for operations management, in which monitoring plays a major role. Consider these four outcomes:

1. Manage cloud production services when they go live into production, such as networking, applications,

security and virtual infrastructure.

2. Apply limited resources to rationalize your existing monitoring tools, skills and expertise, and use cloud monitoring to reduce complexity.
3. Make your monitoring solution processes more efficient, work faster and smoother, at scale and be able to change quickly too.
4. Account for how your organization will plan for and host monitoring based on cloud models. Work towards the goal of reducing your requirements as the organization transitions from IaaS to PaaS, and then to SaaS.

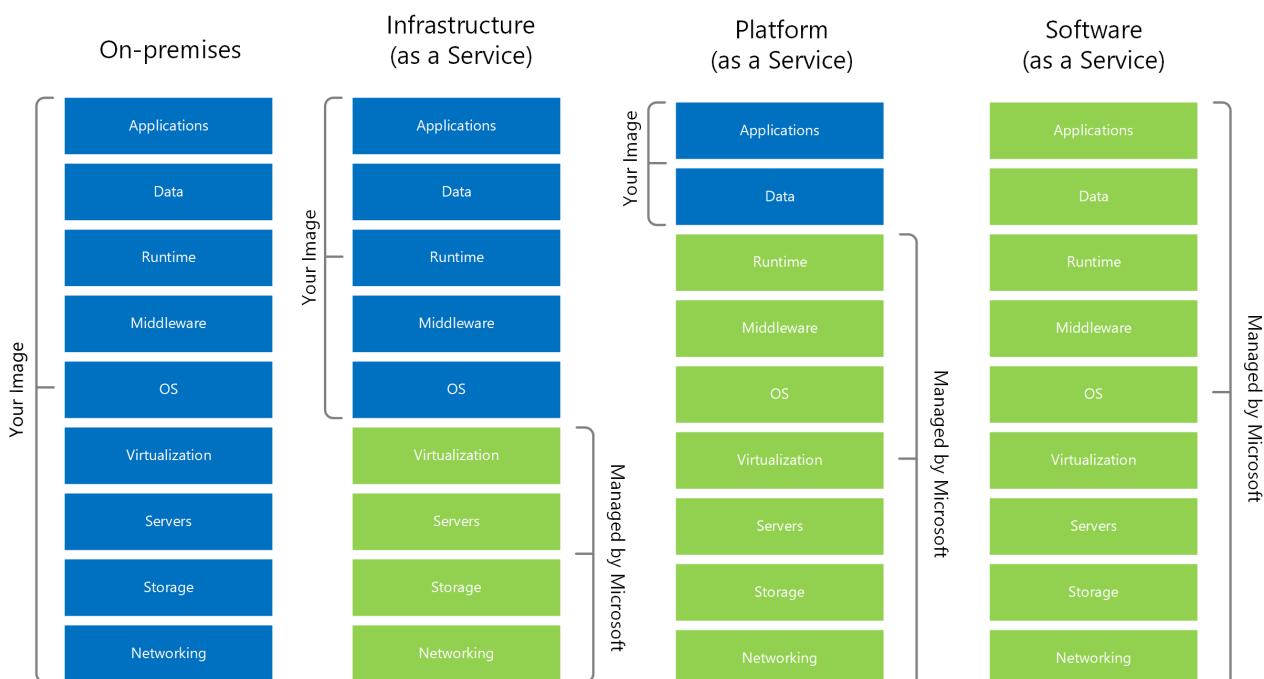
## Determine what you have

As a manageability expert, you may be working closely with a steering committee, an architect, and strategic planners. You might be working to formulate your monitoring strategy by assessing the current state of your systems management, including: the people, partners, outsourcing, tooling, complexity, gaps, and risks. An assessment will help you prioritize the set of found problems and select the key opportunities that improve the current situation. Determine also, the services, systems, and data that are likely to remain on-premises as one important outcome. Ideally, management wants a roadmap of initiatives, but in direct proportion to the known planning horizon. Discussing unknowns, are as important.

## High-level modeling

As the business determines what services to move, you need to invest your resources carefully. On-premises, you own all responsibilities for monitoring and are heavily invested. The moves made toward SaaS services, for example, do not eliminate your monitoring responsibility. You'll decide who needs access, who gets alerts, and who needs access to analytics at a minimum. [Azure Monitor](#) and [Azure Arc](#) are Azure services with the flexibility of addressing monitoring scenarios across all four cloud models, not just resources inside Azure. You need to look beyond the common cloud models as shown below. If you're using Microsoft Office applications delivered by [Microsoft 365](#) services in your organization, you'll need to include security and compliance monitoring with Microsoft 365 in addition to [Azure Security Center](#). This includes identities, endpoint management, and device monitoring outside of your corporate network.

## Cloud Models



# Monitoring informs strategy

Consider where early monitoring capability *informs strategy*. Many decisions depend on early monitoring data in order to build a capability roadmap that guides limited resources and adds confidence. Strategies also need real-world input from monitoring of service enablement.

Consider the role monitoring plays in strategies to incrementally protect and secure the digital estate:

- Activity logs and security monitoring are needed to measure directory usage and external sharing of sensitive content, to inform in an incremental approach to layer on protective features and achieve the right balance with privacy monitoring.
- Policies and baselines will inform the rationalization objective (migrate, lift and shift, or rearchitect) and improve confidence that data and information can be migrated from on-premises to cloud services.

Later in this guide, discover some common monitoring scenarios or use cases that will help accelerate adoption.

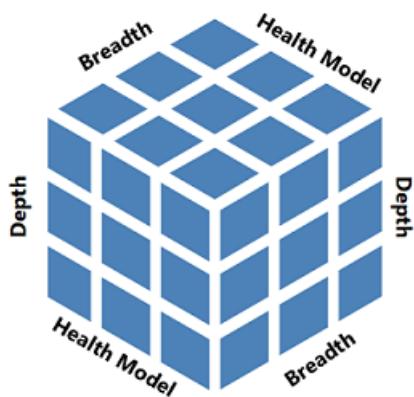
## Formulate a monitoring architecture

Define your current and future architecture of systems management that includes monitoring, to:

- Apply limited resources in consolidating your monitoring investment.
- Decide how monitoring will help enable the future services your business needs: cloud monitoring of highly scalable, resilient, and globally aware cloud services.
- Align monitoring to the future services and resources that you will be monitoring in the cloud.
- Identify monitoring gaps across the three dimensions (depth, breadth, and across) of the health model.
- Model the financial aspects, costs, and support factors that support a cost-benefit analysis.
- Guide the hybrid decisions that you need to make.

One principle of monitoring is service visibility. For a service, asset or component to be fully visible, you need to balance the three sides of this principle, which are:

1. Monitoring in-depth by collecting meaningful and relevant signals.
2. Monitor end-to-end or breadth from the lowest layer of the stack up to the application.
3. East to west with a focus on its aspects of health (availability, performance, security, and continuity).



Some key questions include:

- How will you shape security logs and secure their access back to security and new privacy controls?
- Which services will be globally available and as such, can be globally monitored at the service edge?

- What about the network points between your network infrastructure, and network connectivity to service and application endpoints that tells us when it's us or the cloud provider?
- What are the boundaries of security operations versus health and performance? How can we provide summaries of health and status to security operations, as well as the converse, back to service owners?

To assemble this architecture, here are several considerations:

- A dataflow approach starting from service assets and going up the stack: metrics and log data emitted by infrastructure, IoT devices, mobile devices, and others. Are all of the items under management—to-monitoring tools (mid-tier)? Move upward and outward (ITSM tools, global monitoring, security information and event management (SIEM), custom alert enrichment, and others).
- Whether to continue with [System Center Operations Manager](#) or other monitoring tools.
- The economic cost.
- How the business will use logs and metrics. Azure Monitor brings a significant volume of log and time-series data to the performance and health side of monitoring, similar to what security operations experiences. Logs and metrics are two major data components of the Azure Monitor architecture. The reasons why this is important:
  1. Since you can build large-scale complex cloud services, your problem management costs are reduced to analyze, correlate, and determine causes of problems in one place reducing the need to access resources directly, thereby improving security.
  2. Similar to a SIEM, Azure Monitor is consolidating machine data directly from on-premises assets as well as Azure resources (including activity logs, tenant and subscription data, and any log data from a REST client), and provides a simple query language to provide data analysis far beyond what was possible before.

Consider your data flows and tools:

- Sources and types (telemetric, traces, stateful, time series).
- Tools and suites (rows): (Columns: availability, capacity, security, continuity, and compliance).
- The role of global monitoring or the top-tier.
- The role of IT service management (ITSM) integration to trigger on significant events.

Consider a single policy in your governance plan for event significance, throughout your enterprise, to drive alerting and notifications. It is one of the key policies in your monitoring strategy. The following table is an example of incident management priority model to standardize events, significance, and alerting used for notifications.

Priority		Impact			
		Extensive	Significant	Moderate	Minor
Urgency	Sev 0 - Critical	Critical	Critical	Error	Error
	Sev 1 = Error	Critical	Error	Error	Warning
	Sev 2= Warning	Error	Error	Warning	Warning
	Sev 3 = Informational	Low	Low	Low	Low

## Formulate initiatives

As a monitoring expert or systems administrator, you've discovered that cloud monitoring is faster and easier to

establish, leading to inexpensive demos or proofs-of-value. To overcome the tendency to stay in demo mode, you need to stay in constant touch with strategy and be able to execute on production-focused monitoring plans. Because strategy has plenty of uncertainty and unknowns, you won't know all of the monitoring requirements in advance. Therefore, decide on the first set of adoption plans, based on what is minimally viable to the business and IT management. You may call this a core capability - *that which is needed to begin the journey*. Here are two example initiatives that help declare forward motion:

- Initiative 1: *to reduce the diversity and complexity of our current monitoring investment, we will invest in establishing a core capability using Azure Monitor first, given the same skills and readiness applies to other areas of cloud monitoring.*
- Initiative 2: *to decide on how we use our license plans for identity, access, and overall information protection, we will help the security and privacy offices establish early activity monitoring of users and content as they migrate to the cloud, to clarify questions on classification labels, data loss prevention, encryption, and retention policies.*

### **Consider scale**

Consider scale in your strategy and who will be defining and standardizing *monitoring as code*. Your organization should plan to build standardized solutions using a combination of tools such as:

- Azure Resource Manager templates.
- Azure Policy monitoring initiative definitions and policies.
- GitHub to establish a source control for the scripts, code, and documentation.

### **Consider privacy and security**

In Azure, you'll need to secure certain monitoring data emitted by resources and the control plane actions that are logged in Azure, known as activity logs. Additionally, specialized logs that record user activity such as the Azure Active Directory sign-in and audit logs, and if integrated, the Microsoft 365 unified audit log, as they contain sensitive data that may need to be protected under privacy laws.

Your monitoring strategy should include these components:

- Separate non-monitoring data from monitoring data
- Restrict access to resources

### **Consider business continuity**

Azure Monitor collects, indexes, and analyzes real-time machine and resource-generated data to support your operations and help drive business decisions. Under rare circumstances, it is possible that facilities in an entire region can become inaccessible, for example due to network failures. Or facilities can be lost entirely, for example due to a natural disaster. By relying on these services in the cloud, your planning isn't focused around infrastructure resiliency and high availability, rather its planning for:

- Availability for data ingestion from all your dependent services and resources in Azure, resources in other clouds, and from on-premises.
- Data availability for insights, solutions, workbooks and other visualizations, alerting, integration with ITSM, and other control plane services in Azure supporting your operational requirements.

Create a recovery plan, and make sure that it covers data restoration, network outages, dependent service failures, and region-wide service disruptions.

### **Consider maturity**

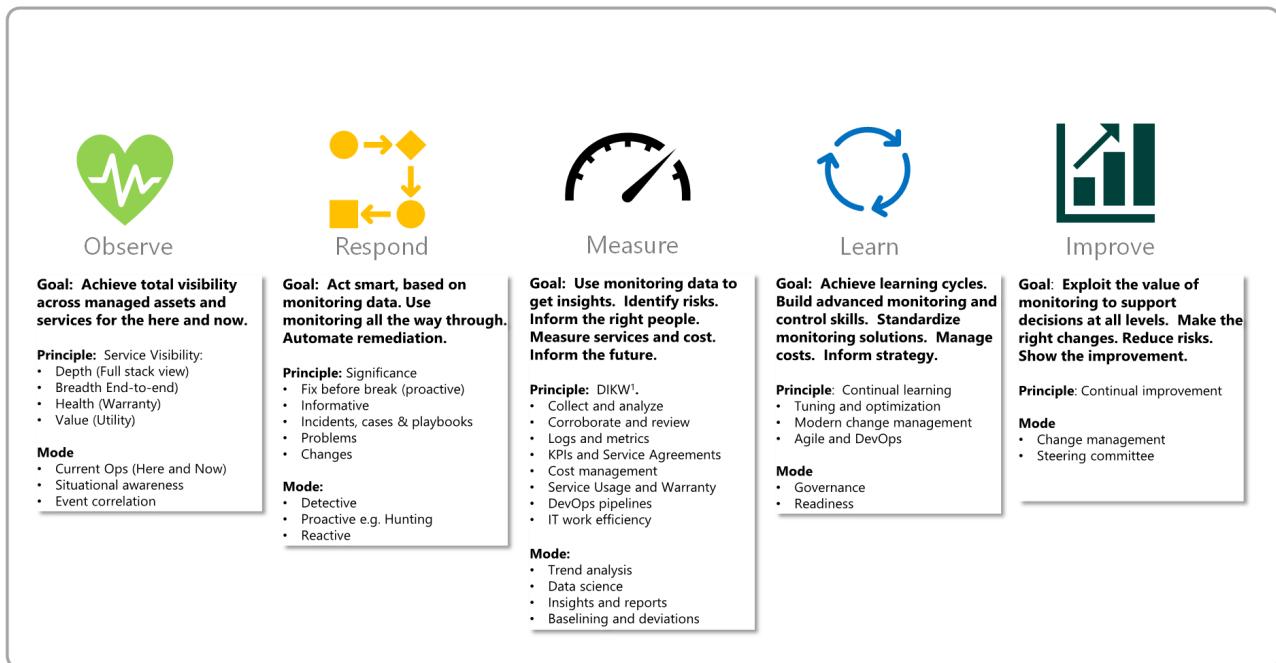
Maturity is an important consideration in your monitoring strategy. We recommend you start minimally, gather data and with this information, determine the strategy. The first monitoring solutions you'll want are those that ensure observability, to include responsive processes, such as incident and problem management. Here, you will:

- Create one or more Log Analytics workspaces

- Enable agents
- Enable resource diagnostic settings
- Enable initial alert rules

Over time, you gain confidence in Azure Monitor capabilities with the need to measure health indicators, so this involves expanding the focus on the collection of logs, enabling and using insights and metrics, and defining log search queries that drive the measurement and calculation of what is healthy or unhealthy.

Learning cycles includes getting monitoring data and insights into the hands of managers, and ensuring the right consumers have monitoring data they need. Learning cycles include continual tuning and optimizing of your initial monitoring plans to adapt, to improve service, and inform adoption plans.



<sup>1</sup> The dikw model is an often used method, with roots in knowledge management, to explain the ways we move from Data to Information, Knowledge, and Wisdom with a component of actions and decisions.

Monitoring is foundational for services you build in Azure. Your strategy can address these four disciplines of modern monitoring, to help you define minimum viable monitoring, and gain confidence in steps. Moving your capability from reactive to proactive and scaling its reach to end users is but one goal.

- **Observe:** First, you should focus on establishing monitoring to observe the health and status of Azure services and resources. Configure basic monitoring and then automate with Azure Policy and Azure Resource Manager templates, to establish initial visibility of services and their warranty: availability, performance or capacity, security, and configuration compliance. For example, based on minimum viable setup of Azure Monitor, configure resources for monitoring and diagnostics, set up alerts, and insights. Include knowledge and readiness of monitoring consumers, defining and triggering from events, for service work such as incidents and problems. One indicator of maturity is how much can be automated to reduce unnecessary human costs to manually observe health and status. Knowing which services are healthy is as important as being alerted on services that are unhealthy.
- **Measure:** Configure collection of metrics and logs from all resources to monitor for symptoms/conditions that are issues, which indicate potential or actual impact to the availability of the service, or impact of the consumers of the service/application. For example:
  - When using a feature in the application, is it showing response time latency, returning an error when I selected something, or unresponsive?
  - Ensure services are meeting service agreements by measuring the utility of the service or application.

- **Respond:** Based on the context of known issues to observe and measure, evaluate what qualifies as a bug, auto-remediation, or requires manual response based on what is classified as an incident, problem, or change.
- **Learn and improve:** Providers and consumers participating in learning cycles implies consuming actual monitoring data through insights, reports and workbooks, to continually improve the target service and to enact tuning and optimization of the monitoring configuration. Change is important too, that the monitoring configuration is changing in tandem with changes to the service (such as new, modified, or retired) and continues to match the actual service warranty.

To help you align monitoring plans to strategy, use the following table to categorize the different monitoring scenarios that occur in more detail. This works with the five Rs of rationalization introduced earlier in the Plan phase. If you're using System Center Operations Manager, you have hybrid and cloud options available to rationalize your investment.

TYPE	MONITORING OBJECTIVE	EXAMPLE OBJECTIVE
1	Only on-premises	System Center Operations Manager. Continue to monitor services, infrastructure, networking up the application layer in owned datacenters with no cloud considerations.
2	On-premises to the cloud	Continue using System Center Operations Manager, and apply the Microsoft 365 and Azure management packs.
3	On-premises to/with cloud (cooperative) where services run in both the cloud and on-premises	Establish initial monitoring with Azure Monitor. Connect Azure Monitor to System Center Operations Manager and alert sources, such as zabbix or nagios. Deploy Azure Monitor monitoring agents, multihoming with System Center Operations Manager where they monitor cooperatively.
4	Hybrid migration	Monitor the migration, for example, Microsoft Exchange Server to Microsoft 365 Exchange Online. Exchange Online service health and service usage, security and compliance, all from Microsoft 365. Gradually decommission monitoring exchange on-premises with System Center Operations Manager until migration is complete.
5	Hybrid forever	System Center Operations Manager, Azure AD, Azure Monitor, Azure Security Center, Intune, and others; a range of tools for a mixture of digital assets.
6	Cloud native	Azure Monitor, Azure Policy, Azure Security Center, Microsoft 365, Azure Service Health, Azure resource health, and others.

Type	Monitoring Objective	Example Objective
7	Multicloud owned tenants (consolidate)	Centralize the monitoring of many tenants. Azure Lighthouse, Azure Policy, Azure Monitor, and Azure Sentinel.
8	Multicloud ecosystem	Centralize the monitoring of different cloud providers: Microsoft, Amazon, Google, and others.
9	Provider > Consumer	Monitoring solutions and services as a cloud provider.

## Formulate monitoring requirements

As you progress through this process, your strategy reveals there may be much to do in the long run. Ultimately your mindset extends outside the corporate network into the workplace, to devices and endpoints, and further outward to the identity-as-security boundary. The new edge defined with cloud monitoring is a strong motivator in contrast with a datacenter and workplace mindset.

You can use Azure now to gradually begin managing all or some aspects of your on-premises resources, even for services you'll keep on-premises. You also want strategy to define your monitoring boundaries of responsibility in alignment with the business' cloud adoption strategy, based on the cloud service model your business adopts. Even for services based on IaaS, you'll get metrics, logs, views, and alerting capabilities through Azure Service Health and here, you'll configure alerts from availability monitoring of your Azure resources with resource health. With SaaS services, such as Microsoft 365, much is already provided, and you need to configure appropriate access to portals, dashboards, analytics, and alerts. From a service perspective, a large service with distributed components such as Microsoft 365 Exchange Online have a number of objectives, not just the need to observe its health and status.

Primary Objective	Goal and Outcome
Health and status monitoring	Holistically observe, measure, learn, and improve the long-term warranty of the service or component, including service levels, in these aspects taken together: availability, capacity, performance, security, and compliance. A healthy system, service or component is online, performing well, secure and compliant. Health monitoring includes logs and is stateful with real-time health states and metrics. It also includes trending reports, insights, and trends focused on service usage.
Utility monitoring	Observe, measure, learn, and improve the quality or qualitative aspects of how a system delivers value. User experience is one type of monitoring use case.
Security monitoring	Observe, measure, learn, and improve protection in support of cybersecurity strategy and functions such as security operations, identity and access, information protection, privacy, threat management and compliance. Monitor using Azure Security Center and Azure Sentinel, as well as Microsoft 365.
Cost monitoring	Monitor usage and estimate costs using Azure Monitor and Azure Cost Management + Billing as a new primary objective. The Azure Cost Management + Billing APIs provide the ability to explore cost and usage data using multidimensional analysis.

TERTIARY OBJECTIVES	GOAL AND OUTCOME
Activity monitoring	Observe, measure, learn, and improve usage, security, and compliance from sources such as Azure activity logs, audit logs, and the Microsoft 365 unified audit log for subscription level events, actions on resources, user and administrator activity, content, data, and for your security and compliance needs in Azure and Microsoft 365.
Service usage	Service owners want analytics and insights to measure, learn, and improve the usage of Azure and Microsoft 365 services (IaaS, PaaS, SaaS) with service usage reports, analytics, and insights. Ensure plans include who will need access to the admin portals, dashboards, insights, and reports.
Service and resource health	Observe the health of your cloud resources, as well as service outages and advisories from Microsoft, to stay informed about incidents and maintenance. Include resource health in monitoring of the availability of your resources and alert on changes in availability.
Capacity and performance monitoring	In support of health monitoring, your needs may require more depth and specialization.
Change and compliance monitoring	Observe, measure, learn, and improve configuration management of resources, which should now include security in the formulation, influenced by good use of Azure Policy to standardize monitoring configurations and enforce security hardening. Log data to filter on key changes being made on resources.
Identity and access monitoring	Observe, measure, learn, and improve both the usage and security of Active Directory, Azure Active Directory, and identity management that integrates users, applications, devices, and other resources no matter where they are.
Information protection	Not only Azure Monitor, but Azure Information Protection depending on the plan, includes usage analytics critical to your development of a robust information protection strategy across Azure and Microsoft.
Privacy monitoring	Organizations face expanding privacy needs to include information protection of the digital estate, data classification, and data loss prevention to mitigate risks to privacy breaches and infractions. Microsoft 365 information protection includes monitoring capabilities that can also be integrated with Azure Monitor.
Threat management and integrated threat protection	The cloud brings together the separate, traditional roles of security monitoring with health monitoring. Integrated threat protection, for example, involves monitoring to accelerate an optimal state of zero trust. Integrating Azure Advanced Threat Protection allows a migration from using System Center Operations Manager to monitor Active Directory, and integrate your Active Directory security-related signals to detect advanced attacks in hybrid environments.

## Agile solution releases

Ultimately, you'll deliver monitoring configurations or solutions into production. As an IT Operations Manager or monitoring team lead, consider a standard, simple taxonomy to improve communication with consumers, managers, and IT operations. An agile DevOps approach ensures monitoring is embedded within the teams who will be building and operating cloud services. While traditional project management works, it is not fast enough nor typically accepted as a standard practice by operations teams.

Include in your strategy and operating model how you communicate monitoring plans, objectives, and configurations (the solutions). For example, how you might use Azure Boards:

AGILE TERM	WHAT TO INCLUDE	EXAMPLES
Epics	Broad monitoring Initiatives of the monitoring strategy	Consolidate Azure cloud monitoring Hybrid cloud monitoring Private cloud monitoring Establish core monitoring service
Features	Individual monitoring Plans and projects	Monitoring requirements Monitoring consumers and providers Objectives Tools Schedule
User stories and tasks	The end result is a monitoring configuration or solution	Network monitoring (for example, ExpressRoute) Standardized IaaS VM monitoring (for example Azure Monitor for VMs, Application Insights, Azure Policy, settings, policies, reports, workspaces.)

## Establish minimum governance

As early as possible, establish how you intend to govern your cloud monitoring investment. Remember that Azure Monitor is a *tenant* service with visibility across management groups and subscriptions, and users can be scoped to limit their actions with Azure role-based access control.

Define who will have what level of access in Azure to support their role and responsibility. We recommend you to set `Reader` role access for monitoring consumers as early as possible and then start controlling who are granted the `Contributor` role.

First, identify the roles who will own and manage resource groups in Azure as part of your governance framework:

- Whether a monitoring team or one or more administrators of resources and resource groups will have privileged access to the `Monitoring Contributor` role.
- The consumers who should be granted the `Monitoring Reader` role, which enables access to features in Azure Monitor, as well as investigate issues within the monitoring section that is included with each Azure resource.
- What managers require access to other Azure reader roles such as `Reports Reader`.

In summary your monitoring consumer roles probably need broad access, versus your developers and system administrators who only need role-based access to certain Azure resources. As an additional restriction, ensure you exempt readers from access to sensitive monitoring data such as security, sign-in and user activity logs.

## Establish readiness

Early on, formulate a readiness plan to help your IT staff adopt new skills, practices, and techniques for cloud

monitoring in Azure. Consider the [skills readiness guidance](#) for monitoring that includes foundational needs, as well as those specific to monitoring.

# Responsible AI

11/9/2020 • 2 minutes to read • [Edit Online](#)

Driven by ethical principles that put people first, Microsoft is committed to advancing AI. We want to partner with you to support this endeavor.

## Responsible AI principles

As you implement AI solutions, consider the following principles in your solution:

- **Fairness:** AI systems should treat all people fairly.
- **Reliability and safety:** AI systems should perform reliably and safely.
- **Privacy and security:** AI systems should be secure and respect privacy.
- **Inclusiveness:** AI systems should empower everyone and engage people.
- **Transparency:** AI systems should be understandable.
- **Accountability:** People should be accountable for AI systems.

## Establish a responsible AI strategy

Learn how to develop your own responsible AI strategy and principles based on the values of your organization.

- [Get started at AI Business School](#)

## Guidelines to develop AI responsibly

Put responsible AI into practice with these guidelines, designed to help you anticipate and address potential issues throughout the software development lifecycle.

- [Human-AI interaction guidelines](#)
- [Conversational AI guidelines](#)
- [Inclusive design guidelines](#)
- [AI fairness checklist](#)
- [Datasheets for datasets template](#)
- [AI security engineering guidance](#)

## Tools for responsible AI

Tools are available to help developers and data scientists understand, protect, and control AI systems. These tools can come from a variety of sources, including Azure Machine Learning, open-source projects, and research.

- **Understand:** AI systems can behave unexpectedly for a variety of reasons. Software tools can help you understand the behavior of your AI systems so that you can better tailor them to your needs. Examples of this type of tool include InterpretML and Fairlearn.
- **Protect:** AI systems rely on data. Software tools can help you protect that data by preserving privacy and ensuring confidentiality. Examples of this type of tool include confidential computing for machine learning, white noise differential privacy, seal homomorphic encryption, and Presidio.
- **Control:** Responsible AI needs governance and control through the development cycle. Azure Machine Learning enables an audit trail for better traceability, lineage, and control to meet regulatory requirements. Examples include audit trail and traceability.

## Next steps

For further resources to support your responsible solution development, visit:

- [Responsible AI overview](#)
- [Responsible AI resources](#)
- [Responsible bots: 10 guidelines for developers of conversational AI](#)

# Skills readiness path during the Plan phase of a migration journey

11/9/2020 • 4 minutes to read • [Edit Online](#)

During the Plan phase of a migration journey, the objective is to develop the plans necessary to guide migration implementation. This phase requires a few critical skills, including:

- Establishing the vision.
- Building the business justification.
- Rationalizing the digital estate.
- Creating a migration backlog (technical plan).

The following sections provide learning paths to develop each of these skills.

## Establish the vision

The success of any cloud adoption effort is defined by the business vision. When the technical team doesn't understand the motives and desired outcomes, it's hard for them to guide their efforts toward business success. See these articles for information about documenting and articulating the business vision for the technical team:

- [Adoption motivations](#). Document and articulate the reasons behind the technical effort.
- [Business outcomes](#). Clearly articulate what's expected of the technical team in terms of business changes.
- [Learning metrics](#). Establish short-term metrics that can show progress toward longer-term business outcomes.

## Build the business justification

Justifying the investment to adopt the cloud can require deeper analysis and an understanding of your organization's accounting practices. The articles on business justification can help you develop these skills:

- [Cloud migration business case](#). Establish a business case for cloud migration.

## Rationalize the digital estate

You can refine your business case by aligning the desired business case with current and future digital estate inventory. These articles can guide the development of a digital estate rationalization:

- [Incremental rationalization](#): An agile approach to rationalization that properly aligns late-bound technical decisions.
- The [five Rs of rationalization](#): Understand the various rationalization options.

## Create a migration backlog (technical plan)

Convert the business case and rationalized digital estate into an actionable migration plan to guide the technical activities required to achieve the desired business outcomes.

## Business planning skills

During the Ready phase, technical staff creates a migration landing zone capable of hosting, operating, and governing workloads that have been migrated to the cloud. These learning paths can help you develop the necessary skills:

- [Create an Azure account](#). The first step to using Azure is to create an account. Your account holds the Azure services you provision and handles your personal settings, like identity, billing, and preferences.
- [Azure portal](#). Tour the Azure portal features and services, and customize the portal.
- [Introduction to Azure](#). Get started with Azure by creating and configuring your first virtual machine in the cloud.
- [Introduction to security in Azure](#). Learn the basic concepts for protecting your infrastructure and data when you work in the cloud. Understand what responsibilities are yours and what Azure takes care of for you.
- [Manage resources in Azure](#). Learn how to work with the Azure command line and web portal to create, manage, and control cloud-based resources.
- [Create a VM](#). Create a virtual machine by using the Azure portal.
- [Azure networking](#). Learn the basics of Azure networking and how Azure networking helps you improve resiliency and reduce latency.
- [Azure compute options](#). Learn about the Azure compute services.
- [Secure resources with RBAC](#). Use RBAC to secure resources.
- [Data storage options](#). Learn about the benefits of Azure data storage.

## Organizational skills

Depending on the motivations and desired business outcomes of a cloud adoption effort, leaders might need to establish new organizational structures or virtual teams to facilitate various functions. These articles will help you develop the skills necessary to structure those teams to meet desired outcomes:

- [Initial organizational alignment](#). Overview of organizational alignment and various team structures to facilitate specific goals.
- [Breaking down silos and fiefdoms](#). Understanding two common organizational antipatterns and ways to guide a team to productive collaboration.

## Deeper skills exploration

Beyond these initial options for developing skills, a variety of learning options is available.

### Typical mappings of cloud IT roles

Microsoft and partners offer various options to help all audiences develop their skills with Azure services:

- [Microsoft IT Pro Center](#). Serves as a free online resource to help map your cloud career path. Learn what industry experts suggest for your cloud role and the skills to get you there. Follow a learning curriculum at your own pace to build the skills you need most to stay relevant.

We recommend turning knowledge of Azure into official recognition with [Microsoft Azure certification training and exams](#).

## Microsoft Learn

Microsoft Learn is a new approach to learning. Readiness for the new skills and responsibilities that come with cloud adoption doesn't come easily. Microsoft Learn provides a more rewarding approach to hands-on learning that helps you achieve your goals faster. Earn points and levels, and achieve more!

Here is an example of a tailored learning path that aligns to the Strategy methodology of the Cloud Adoption Framework.

[Learn the business value of Microsoft Azure](#): This learning experience will take you on a journey that will begin by showing you how digital transformation and the power of the cloud can transform your business. We will cover how Microsoft Azure cloud services can power your organization on a trusted cloud platform. Finally, we will wrap up by illustrating how to make this journey real for your organization.

## Learn more

To discover additional learning paths, browse the [Microsoft Learn catalog](#). Use the **Roles** filter to align learning paths with your role.

# Develop a cloud adoption plan

11/9/2020 • 2 minutes to read • [Edit Online](#)

Cloud adoption plans convert the aspirational goals of a cloud adoption strategy into an actionable plan. The collective cloud teams can use the cloud adoption plan to guide their technical efforts and align them with the business strategy.

The following exercises will help you document your technology strategy. This approach captures prioritized tasks to drive adoption efforts. The cloud adoption plan then maps to the metrics and motivations defined in the cloud adoption strategy.

1	<p><b>Digital estate:</b> Inventory and rationalize your digital estate based on assumptions that align with motivations and business outcomes.</p>
2	<p><b>Initial organizational alignment:</b> Establish a plan for initial organizational alignment to support the adoption plan.</p>
3	<p><b>Skills readiness plan:</b> Create a plan for addressing skills readiness gaps.</p>
4	<p><b>Cloud adoption plan:</b> Develop a cloud adoption plan to manage change across the digital estate, skills, and organization.</p>

Download the [strategy and plan template](#) to track the outputs of each exercise as you build out your cloud adoption strategy. Also, learn about the [five Rs of cloud rationalization](#) to help build your cloud adoption plan.

# Cloud rationalization

11/9/2020 • 4 minutes to read • [Edit Online](#)

Cloud rationalization is the process of evaluating assets to determine the best way to migrate or modernize each asset in the cloud. For more information about the process of rationalization, see [What is a digital estate?](#).

## Rationalization context

The *five Rs of rationalization* listed in this article are a great way to label a potential future state for any workload that's being considered as a cloud candidate. This labeling process should be put into the correct context before you attempt to rationalize an environment. Review the following myths to provide that context:

### **Myth: It's easy to make rationalization decisions early in the process**

Accurate rationalization requires a deep knowledge of the workload and associated assets (applications, infrastructure, and data). Most importantly, accurate rationalization decisions take time. We recommend using an [incremental rationalization process](#).

### **Myth: Cloud adoption has to wait for all workloads to be rationalized**

Rationalizing an entire IT portfolio or even a single datacenter can delay the realization of business value by months or even years. Full rationalization should be avoided when possible. Instead, use the [Power of 10 approach to release planning](#) to make wise decisions about the next 10 workloads that are slated for cloud adoption.

### **Myth: Business justification has to wait for all workloads to be rationalized**

To develop a business justification for a cloud adoption effort, make a few basic assumptions at the portfolio level. When motivations are aligned to innovation, assume rearchitecture. When motivations are aligned to migration, assume rehost. These assumptions can accelerate the business justification process. Assumptions are then challenged and budgets refined during the Assess phase of each workload's adoption cycles.

Now review the following five Rs of rationalization to familiarize yourself with the long-term process. While developing your cloud adoption plan, choose the option that best aligns with your motivations, business outcomes, and current state environment. The goal in digital estate rationalization is to set a baseline, not to rationalize every workload.

## The five Rs of rationalization

The five Rs of rationalization that are listed here describe the most common options for rationalization.

### Rehost

Also known as a *lift and shift* migration, a rehost effort moves a current state asset to the chosen cloud provider, with minimal change to overall architecture.

Common drivers might include:

- Reducing capital expense.
- Freeing up datacenter space.
- Achieving rapid return on investment in the cloud.

Quantitative analysis factors:

- VM size (CPU, memory, storage).

- Dependencies (network traffic).
- Asset compatibility.

Qualitative analysis factors:

- Tolerance for change.
- Business priorities.
- Critical business events.
- Process dependencies.

## Refactor

Platform as a service (PaaS) options can reduce the operational costs that are associated with many applications. It's a good idea to slightly refactor an application to fit a PaaS-based model.

"Refactor" also refers to the application development process of refactoring code to enable an application to deliver on new business opportunities.

Common drivers might include:

- Faster and shorter updates.
- Code portability.
- Greater cloud efficiency (resources, speed, cost, managed operations).

Quantitative analysis factors:

- Application asset size (CPU, memory, storage).
- Dependencies (network traffic).
- User traffic (page views, time on page, load time).
- Development platform (languages, data platform, middle-tier services).
- Database (CPU, memory, storage, version).

Qualitative analysis factors:

- Continued business investments.
- Bursting options or timelines.
- Business process dependencies.

## Rearchitect

Some aging applications aren't compatible with cloud providers because of the architectural decisions that were made when the application was built. In these cases, the application might need to be rearchitected before transformation.

In other cases, applications that are cloud-compatible, but not cloud-native, might create cost efficiencies and operational efficiencies by rearchitecting the solution into a cloud-native application.

Common drivers might include:

- Application scale and agility.
- Easier adoption of new cloud capabilities.
- Mix of technology stacks.

Quantitative analysis factors:

- Application asset size (CPU, memory, storage).

- Dependencies (network traffic).
- User traffic (page views, time on page, load time).
- Development platform (languages, data platform, middle tier services).
- Database (CPU, memory, storage, version).

Qualitative analysis factors:

- Growing business investments.
- Operational costs.
- Potential feedback loops and DevOps investments.

## Rebuild

In some scenarios, the delta that must be overcome to carry an application forward can be too large to justify further investment. This is especially true for applications that previously met the needs of a business but are now unsupported or misaligned with the current business processes. In this case, a new code base is created to align with a [cloud-native](#) approach.

Common drivers might include:

- Accelerating innovation.
- Building applications faster.
- Reducing operational cost.

Quantitative analysis factors:

- Application asset size (CPU, memory, storage).
- Dependencies (network traffic).
- User traffic (page views, time on page, load time).
- Development platform (languages, data platform, middle tier services).
- Database (CPU, memory, storage, version).

Qualitative analysis factors:

- Declining end-user satisfaction.
- Business processes limited by functionality.
- Potential cost, experience, or revenue gains.

## Replace

Solutions are typically implemented by using the best technology and approach available at the time. Sometimes software as a service (SaaS) applications can provide all the necessary functionality for the hosted application. In these scenarios, a workload can be scheduled for future replacement, effectively removing it from the transformation effort.

Common drivers might include:

- Standardizing around industry best practices.
- Accelerating adoption of business-process-driven approaches.
- Reallocating development investments into applications that create competitive differentiation or advantages.

Quantitative analysis factors:

- General operating-cost reductions.
- VM size (CPU, memory, storage).

- Dependencies (network traffic).
- Assets to be retired.
- Database (CPU, memory, storage, version).

Qualitative analysis factors:

- Cost benefit analysis of the current architecture versus a SaaS solution.
- Business process maps.
- Data schemas.
- Custom or automated processes.

## Next steps

Collectively, you can apply these five Rs of rationalization to a digital estate to help you make rationalization decisions about the future state of each application.

[What is a digital estate?](#)

# What is a digital estate?

11/9/2020 • 2 minutes to read • [Edit Online](#)

Every modern company has some form of digital estate. Much like a physical estate, a digital estate is an abstract reference to a collection of tangible owned assets. In a digital estate, those assets include virtual machines (VMs), servers, applications, data, and so on. Essentially, a digital estate is the collection of IT assets that power business processes and supporting operations.

The importance of a digital estate is most obvious during the planning and execution of digital transformation efforts. During transformation journeys, the cloud strategy teams use the digital estate to map the business outcomes to release plans and technical efforts. That all starts with an inventory and measurement of the digital assets that the organization owns today.

## How can a digital estate be measured?

The measurement of a digital estate changes depending on the desired business outcomes.

- **Infrastructure migrations:** When an organization is inward-facing and seeks to optimize costs, operational processes, agility, or other aspects of their operations, the digital estate focuses on VMs, servers, and workloads.
- **Application innovation:** For customer-focused transformations, the lens is a bit different. The focus should be placed on the applications, APIs, and transactional data that supports the customers. VMs and network appliances often receive less focus.
- **Data-driven innovation:** In today's digitally driven market, it's difficult to launch a new product or service without a strong foundation in data. During cloud-enabled data innovation efforts, the focus is more on the silos of data across the organization.
- **Operational stability:** Businesses are dependent on stable technologies to operate effectively. Near-zero downtime and service reliability are crucial in competitive markets. When operational stability is a priority, the digital estate should be measured on positive or negative impact to stable operations. Business continuity, disaster recovery, and reliability of workloads and each asset are required measures when operational stability is a priority.

After an organization understands the most important form of transformation, digital estate planning becomes much easier to manage.

Each type of transformation can be measured with any of the above views. Companies commonly complete all these transformations in parallel. We strongly recommend that company leadership and the cloud strategy team agree regarding the transformation that is most important for business success. That understanding serves as the basis for common language and metrics across multiple initiatives.

## How can a financial model be updated to reflect the digital estate?

An analysis of the digital estate drives cloud adoption activities. It also informs financial models by providing cloud costing models, which in turn drive return on investment (ROI).

To complete the digital estate analysis, take the following steps:

1. [Determine analysis approach](#).
2. [Collect current state inventory](#).

3. Rationalize the assets in the digital estate.
4. Align assets to cloud offerings to calculate pricing.

Financial models and migration backlogs can be modified to reflect the rationalized and priced estate.

## Next steps

Before digital estate planning begins, determine which approach to use.

[Approaches to digital estate planning](#)

# Approaches to digital estate planning

11/9/2020 • 3 minutes to read • [Edit Online](#)

Digital estate planning can take several forms depending on the desired outcomes and size of the existing estate. There are various approaches that you can take. It's important to set expectations regarding the approach early in planning cycles. Unclear expectations often lead to delays associated with additional inventory-gathering exercises. This article outlines three approaches to analysis.

## Workload-driven approach

The top-down assessment approach evaluates security aspects. Security includes the categorization of data (high, medium, or low business impact), compliance, sovereignty, and security risk requirements. This approach assesses high-level architectural complexity. It evaluates aspects such as authentication, data structure, latency requirements, dependencies, and application life expectancy.

The top-down approach also measures the operational requirements of the application, such as service levels, integration, maintenance windows, monitoring, and insight. When these aspects have been analyzed and considered, the resulting score reflects the relative difficulty of migrating this application to each cloud platform: IaaS, PaaS, and SaaS.

In addition, the top-down assessment evaluates the financial benefits of the application, such as operational efficiencies, TCO, return on investment, and other appropriate financial metrics. The assessment also examines the seasonality of the application (such as whether there are certain times of the year when demand spikes) and overall compute load.

It also looks at the types of users it supports (casual/expert, always/occasionally logged on), and the required scalability and elasticity. Finally, the assessment concludes by examining business continuity and resiliency requirements, as well as dependencies for running the application if a disruption of service should occur.

### TIP

This approach requires interviews and anecdotal feedback from business and technical stakeholders. Availability of key individuals is the biggest risk to timing. The anecdotal nature of the data sources makes it more difficult to produce accurate cost or timing estimates. Plan schedules in advance and validate any data that's collected.

## Asset-driven approach

The asset-driven approach provides a plan based on the assets that support an application for migration. In this approach, you pull statistical usage data from a configuration management database (CMDB) or other infrastructure assessment tools.

This approach usually assumes an IaaS model of deployment as a baseline. In this process, the analysis evaluates the attributes of each asset: memory, number of processors (CPU cores), operating system storage space, data drives, network interface cards (NICs), IPv6, network load balancing, clustering, operating system version, database version (if necessary), supported domains, and third-party components or software packages, among others. The assets that you inventory in this approach are then aligned with workloads or applications for grouping and dependency mapping purposes.

**TIP**

This approach requires a rich source of statistical usage data. The time that's needed to scan the inventory and collect data is the biggest risk to timing. The low-level data sources can miss dependencies between assets or applications. Plan for at least one month to scan the inventory. Validate dependencies before deployment.

## Incremental approach

We strongly suggest an incremental approach, as we do for many processes in the Cloud Adoption Framework. In the case of digital estate planning, that equates to a multiphase process:

- **Initial cost analysis:** If financial validation is required, start with an asset-driven approach, described earlier, to get an initial cost calculation for the entire digital estate, with no rationalization. This establishes a worst-case scenario benchmark.
- **Migration planning:** After you have assembled a cloud strategy team, build an initial migration backlog using a workload-driven approach that's based on their collective knowledge and limited stakeholder interviews. This approach quickly builds a lightweight workload assessment to foster collaboration.
- **Release planning:** At each release, the migration backlog is pruned and reprioritized to focus on the most relevant business impact. During this process, the next five to ten workloads are selected as prioritized releases. At this point, the cloud strategy team invests the time in completing an exhaustive workload-driven approach. Delaying this assessment until a release is aligned better respects the time of stakeholders. It also delays the investment in full analysis until the business starts to see results from earlier efforts.
- **Execution analysis:** Before migrating, modernizing, or replicating any asset, assess it both individually and as part of a collective release. At this point, the data from the initial asset-driven approach can be scrutinized to ensure accurate sizing and operational constraints.

**TIP**

This incremental approach enables streamlined planning and accelerated results. It's important that all parties involved understand the approach to delayed decision making. It's equally important that assumptions made at each stage be documented to avoid loss of details.

## Next steps

After an approach is selected, the inventory can be collected.

[Gather inventory data](#)

# Gather inventory data for a digital estate

11/9/2020 • 2 minutes to read • [Edit Online](#)

Developing an inventory is the first step for [digital estate planning](#). In this process, a list of IT assets that support specific business functions are collected for later analysis and rationalization. This article assumes that a bottom-up approach to analysis is most appropriate for planning. For more information, see [Approaches to digital estate planning](#).

## Take inventory of a digital estate

The inventory that supports a digital estate changes depending on the desired digital transformation and corresponding transformation journey.

- **Cloud migration:** We often recommend that during a cloud migration, you collect the inventory from scanning tools that create a centralized list of all virtual machines and servers. Some tools can also create network mappings and dependencies, which help define workload alignment.
- **Application innovation:** Inventory during a cloud-enabled application innovation effort begins with the customer. Mapping the customer experience from start to finish is a good place to begin. Aligning that map to applications, APIs, data, and other assets creates a detailed inventory for analysis.
- **Data innovation:** Cloud-enabled data innovation efforts focus on the product or service. An inventory also includes a mapping of the opportunities for disrupting the market, as well as the capabilities needed.
- **Security:** Inventory provides security the understanding to help assess, protect, and monitor the organization's assets.

## Accuracy and completeness of an inventory

An inventory is rarely complete in its first iteration. We strongly recommend the cloud strategy team aligns stakeholders and power users to validate the inventory. When possible, use additional tools like network and dependency analysis to identify assets that are being sent traffic, but that are not in the inventory.

## Next steps

After an inventory is compiled and validated, it can be rationalized. Inventory rationalization is the next step to digital estate planning.

[Rationalize the digital estate](#)

# Rationalize the digital estate

11/9/2020 • 10 minutes to read • [Edit Online](#)

Cloud rationalization is the process of evaluating assets to determine the best approach to hosting them in the cloud. After you've determined an [approach](#) and aggregated an [inventory](#), cloud rationalization can begin. Cloud rationalization discusses the most common rationalization options.

## Traditional view of rationalization

It's easy to understand rationalization when you visualize the traditional process of rationalization as a complex decision tree. Each asset in the digital estate is fed through a process that results in one of five answers (the five Rs of rationalization). For small estates, this process works well. For larger estates, it's inefficient and can lead to significant delays. Let's examine the process to see why. Then we'll present a more efficient model.

**Inventory:** A thorough inventory of assets, including applications, software, hardware, operating systems, and system performance metrics, is required for completing a full rationalization by using traditional models.

**Quantitative analysis:** In the decision tree, quantitative questions drive the first layer of decisions. Common questions include the following:

- Is the asset in use today?
- If so, is it optimized and sized properly?
- What dependencies exist between assets? These questions are vital to the classification of the inventory.

**Qualitative analysis:** The next set of decisions requires human intelligence in the form of qualitative analysis. Often, the questions that come up here are unique to the solution and can be answered only by business stakeholders and power users. These decisions typically delay the process, slowing things down considerably. This analysis generally consumes 40 to 80 FTE hours per application.

For guidance about building a list of qualitative analysis questions, see [Approaches to digital estate planning](#).

**Rationalization decision:** In the hands of an experienced rationalization team, the qualitative and quantitative data creates clear decisions. Unfortunately, teams with a high degree of rationalization experience are expensive to hire or take months to train.

## Rationalization at enterprise scale

If this effort is time consuming and daunting for a 50-VM digital estate, imagine the effort that's required to drive business transformation in an environment with thousands of VMs and hundreds of applications. The human effort required can easily exceed 1,500 FTE hours and nine months of planning.

While full rationalization is the end state and a great direction to move in, it seldom produces a high ROI (return on investment) relative to the time and energy that's required.

When rationalization is essential to financial decisions, it's worth considering a professional services organization that specializes in cloud rationalization to accelerate the process. Even then, full rationalization can be a costly and time-consuming effort that delays transformation or business outcomes.

The rest of this article describes an alternative approach, known as incremental rationalization.

## Incremental rationalization

The complete rationalization of a large digital estate is prone to risk and can suffer delays because of its

complexity. The assumption behind the incremental approach is that delayed decisions stagger the load on the business to reduce the risk of roadblocks. Over time, this approach creates an organic model for developing the processes and experience required to make qualified rationalization decisions more efficiently.

### **Inventory: Reduce discovery data points**

Few organizations invest the time, energy, and expense in maintaining an accurate real-time inventory of the full digital estate. Loss, theft, refresh cycles, and employee onboarding often justify detailed asset tracking of end-user devices. The ROI of maintaining an accurate server and application inventory in a traditional, on-premises datacenter is often low. Most IT organizations have more urgent issues to address than tracking the usage of fixed assets in a datacenter.

In a cloud transformation, inventory directly correlates to operating costs. Accurate inventory data is required for proper planning. Unfortunately, current environmental scanning options can delay decisions by weeks or months. Fortunately, a few tricks can accelerate data collection.

Agent-based scanning is the most frequently cited delay. The robust data that's required for a traditional rationalization can often only be collected with an agent running on each asset. This dependency on agents often slows progress, because it can require feedback from security, operations, and administration functions.

In an incremental rationalization process, an agentless solution could be used for an initial discovery to accelerate early decisions. Depending on the level of complexity in the environment, an agent-based solution might still be required, but it can be removed from the critical path to business change.

### **Quantitative analysis: Streamline decisions**

Regardless of the approach to inventory discovery, quantitative analysis can drive initial decisions and assumptions. This is especially true when trying to identify the first workload or when the goal of rationalization is a high-level cost comparison. In an incremental rationalization process, the cloud strategy team and the cloud adoption teams limit the [five Rs of rationalization](#) to two concise decisions and only apply those quantitative factors. This streamlines the analysis and reduces the amount of initial data that's required to drive change.

For example, if an organization is in the midst of an IaaS migration to the cloud, you can assume that most workloads will either be retired or rehosted.

### **Qualitative analysis: Temporary assumptions**

By reducing the number of potential outcomes, it's easier to reach an initial decision about the future state of an asset. When you reduce the options, you also reduce the number of questions asked of the business at this early stage.

For example, if the options are limited to rehosting or retiring, the business needs to answer only one question during initial rationalization, which is whether to retire the asset.

"Analysis suggests that no users are actively using this asset. Is that accurate, or have we overlooked something?" Such a binary question is typically much easier to run through qualitative analysis.

This streamlined approach produces baselines, financial plans, strategy, and direction. In later activities, each asset goes through further rationalization and qualitative analysis to evaluate other options. All assumptions that you make in this initial rationalization are tested before migrating individual workloads.

## **Challenge assumptions**

The outcome of the prior section is a rough rationalization that's full of assumptions. Next, it's time to challenge some of those assumptions.

### **Retire assets**

In a traditional on-premises environment, hosting small, unused assets seldom causes a significant impact on annual costs. With a few exceptions, FTE effort that's required to analyze and retire the actual asset outweighs

the cost savings from pruning and retiring those assets.

When you move to a cloud accounting model, retiring assets can produce significant savings in annual operating costs and up-front migration efforts.

It's not uncommon for organizations to retire 20% or more of their digital estate after completing a quantitative analysis. We recommend conducting further qualitative analysis before taking action. After it's confirmed, retiring those assets can produce the first ROI victory of the cloud migration. This is often one of the biggest cost-saving factors. Therefore, the cloud strategy team should oversee the validation and retirement of assets, in parallel with execution of the [Migrate methodology](#), to achieve an early financial win.

### **Program adjustments**

A company seldom embarks on just one transformation journey. The choice between cost reduction, market growth, and new revenue streams is rarely a binary decision. As such, we recommend that the cloud strategy team work with IT to identify assets on parallel transformation efforts that are outside of the scope of the primary transformation journey.

In the IaaS migration example given in this article:

- Ask the DevOps team to identify assets that are already part of a deployment automation and remove those assets from the core migration plan.
- Ask the data and R&D teams to identify assets that are powering new revenue streams and remove them from the core migration plan.

This program-focused qualitative analysis can be executed quickly and creates alignment across multiple migration backlogs.

You might still need to consider some assets as rehost assets for a while. You can phase in later rationalization after the initial migration.

## Select the first workload

Implementing the first workload is key to testing and learning. It's the first opportunity to demonstrate and build a growth mindset.

### **Business criteria**

To ensure business transparency, identify a workload that is supported by a member of the cloud strategy team's business unit. Preferably choose one in which the team has a vested stake and strong motivation to move to the cloud.

### **Technical criteria**

Select a workload that has minimum dependencies and can be moved as a small group of assets. We recommend that you select a workload with a defined testing path to make validation easier.

The first workload is often deployed in an experimental environment with no operational or governance capacity. It's important to select a workload that doesn't interact with secure data.

### **Qualitative analysis**

The cloud adoption teams and the cloud strategy team can work together to analyze this small workload. This collaboration creates a controlled opportunity to create and test qualitative analysis criteria. The smaller population creates an opportunity to survey the affected users, and to complete a detailed qualitative analysis in a week or less. For common qualitative analysis factors, see the specific rationalization target in the [five Rs of rationalization](#).

### **Migration**

In parallel with continued rationalization, the cloud adoption team can begin migrating the small workload to

expand learning in the following key areas:

- Strengthen skills with the cloud provider's platform.
- Define the core services and Azure standards needed to fit the long-term vision.
- Better understand how operations might need to change later in the transformation.
- Understand any inherent business risks and the business's tolerance for those risks.
- Establish a baseline or minimum viable product (MVP) for governance based on the business's risk tolerance.

## Release planning

While the cloud adoption team is executing the migration or implementation of the first workload, the cloud strategy team can begin prioritizing the remaining applications and workloads.

### Power of 10

The traditional approach to rationalization attempts to meet all foreseeable needs. Fortunately, a plan for every application is often not required to start a transformation journey. In an incremental model, the Power of 10 approach provides a good starting point. In this model, the cloud strategy team selects the first 10 applications to be migrated. Those ten workloads should contain a mixture of simple and complex workloads.

### Build the first backlogs

The cloud adoption teams and the cloud strategy team can work together on the qualitative analysis for the first 10 workloads. This effort creates the first prioritized migration backlog and the first prioritized release backlog. This method enables the teams to iterate on the approach and provides sufficient time to create an adequate process for qualitative analysis.

### Mature the process

After the two teams agree on the qualitative analysis criteria, assessment can become a task within each iteration. Reaching consensus on assessment criteria usually requires two to three releases.

After the assessment has moved into the incremental execution process of migration, the cloud adoption team can iterate faster on assessment and architecture. At this stage, the cloud strategy team is also abstracted, reducing the drain on their time. This also enables the cloud strategy team to focus on prioritizing the applications that are not yet in a specific release, ensuring tight alignment with changing market conditions.

Not all of the prioritized applications will be ready for migration. Sequencing is likely to change as the team does deeper qualitative analysis and discovers business events and dependencies that might prompt reprioritization of the backlog. Some releases might group together a small number of workloads. Others might just contain a single workload.

The cloud adoption team is likely to run iterations that don't produce a complete workload migration. The smaller the workload, and the fewer dependencies, the more likely a workload is to fit into a single sprint or iteration. For this reason, we recommend that the first few applications in the release backlog be small and contain few external dependencies.

## End state

Over time, the cloud adoption team and the cloud strategy team together complete a full rationalization of the inventory. This incremental approach enables the teams to get continually faster at the rationalization process. It also helps the transformation journey to yield tangible business results sooner, without as much upfront analysis effort.

In some cases, the financial model might be too tight to make a decision without additional rationalization. In such cases, you might need a more traditional approach to rationalization.

## Next steps

The output of a rationalization effort is a prioritized backlog of all assets that are affected by the chosen transformation. This backlog is now ready to serve as the foundation for costing models of cloud services.

[Align cost models with the digital estate](#)

# Align cost models with the digital estate to forecast cloud costs

11/9/2020 • 2 minutes to read • [Edit Online](#)

After you've rationalized a digital estate, you can align it to equivalent costing models with the chosen cloud provider. Discussing cost models is difficult without focusing on a specific cloud provider. To provide tangible examples in this article, Azure is the assumed cloud provider.

Azure pricing tools help you manage cloud spend with transparency and accuracy, so you can make the most of Azure and other clouds. Providing the tools to monitor, allocate, and optimize cloud costs, empowers customers to accelerate future investments with confidence.

- [Azure Migrate](#): Azure Migrate is perhaps the most cost effective approach to cost model alignment. This tool allows for [digital estate inventory](#), [limited rationalization](#), and cost calculations in one tool.
- [Total cost of ownership \(TCO\) calculator](#): Lower the total cost of ownership of your on-premises infrastructure with the Azure cloud platform. Use the Azure TCO calculator to estimate the cost savings you can realize by migrating your application workloads to Azure. Provide a brief description of your on-premises environment to get an instant report.
- [Azure pricing calculator](#): Estimate your expected monthly bill by using our pricing calculator. Track your actual account usage and bill at any time using the billing portal. Set up automatic email billing alerts to notify you if your spend goes above an amount you configure.
- [Azure Cost Management + Billing](#): Azure Cost Management + Billing is a cost management solution that helps you use and manage Azure and other cloud resources effectively. Collect cloud usage and billing data through application program interfaces (APIs) from Azure, Amazon Web Services, and Google Cloud Platform. With that data, gain full visibility into resource consumption and costs across cloud platforms in a single, unified view. Continuously monitor cloud consumption and cost trends. Track actual cloud spending against your budget to avoid overspending. Detect spending anomalies and usage inefficiencies. Use historical data to improve your forecasting accuracy for cloud usage and expenditures.

# Measure business outcomes with AppDynamics

11/9/2020 • 4 minutes to read • [Edit Online](#)

Measuring and quantifying successful business outcomes is a crucial part of any cloud adoption strategy. Understanding an application's performance and user experience is key to measuring those business outcomes. However, accurately measuring the correlation between application performance, user experience, and business impact is often difficult, inaccurate, and time consuming.

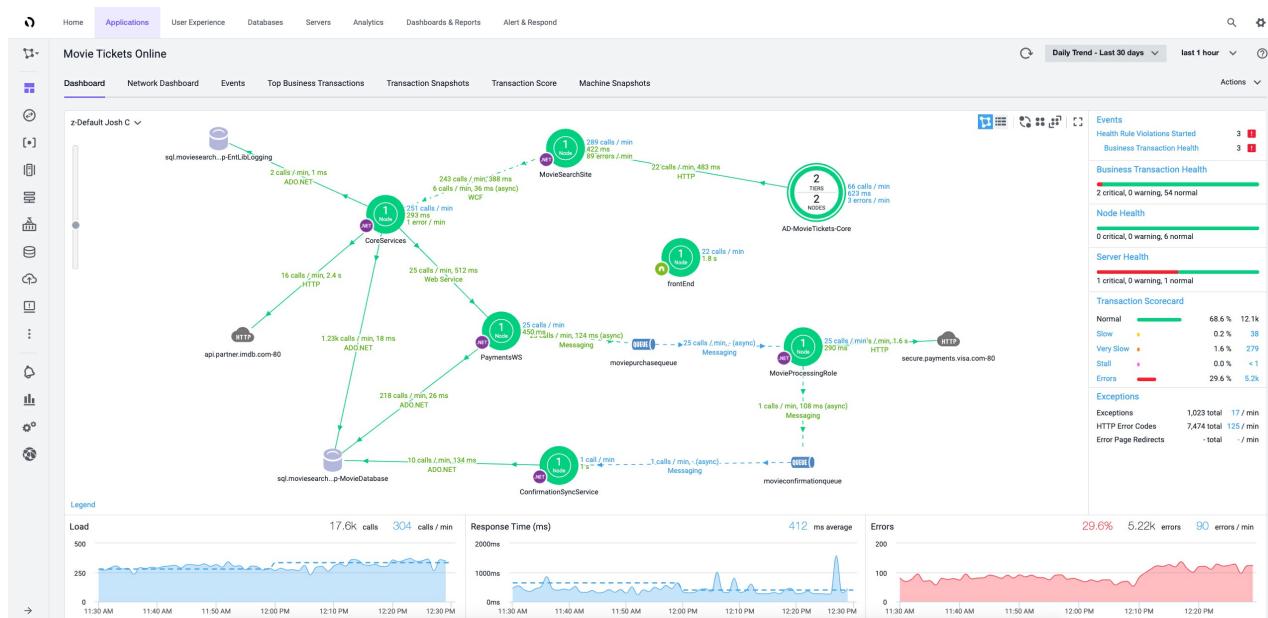
AppDynamics can provide business insights for most use cases, and many organizations start a comprehensive cloud adoption strategy with the following use cases:

- A pre- and post-migration comparison
  - Business health
  - Release validation
  - Segment health
  - User journeys
  - Business journeys
  - Conversion funnels

This guidance will focus on how to measure business outcomes of a pre- and post-migration comparison and how to accelerate and reduce risk for a migration during your cloud adoption journey.

## How AppDynamics works

Prior to migration, a small, lightweight agent is deployed alongside your applications. Agents are purpose-built for various languages such as .NET, Java, and Node.js. The agent collects performance and diagnostic data during the migration and sends it to a controller to correlate and analyze the information. Controllers can reside in a fully managed AppDynamics environment, or the customer can choose to manage them in Azure. Key user experiences are identified as 'business transactions', which help you to discover the baseline for normal application or business performance. Whether they're traditional server infrastructure, database, middleware components, on-premises, or in the cloud, all application components and dependencies are identified in real time for the entire application and each business transaction.



*Figure 1: An AppDynamics flow map.*

## AppDynamics identifies business metrics

AppDynamics helps you to define business value for your applications, identify the key metrics that they should meet to retain their value, and verify if they're fulfilling their target business outcomes. AppDynamics agents collect these data points and traditional application performance metrics like response time and memory utilization in real time, directly from the application, and without any changes to code.

Business metrics are closely related to business outcomes. Many organizations have complex metrics that measure unique business outcomes, and these outcomes can range from fiscal and agility-related to performance and customer engagement goals. AppDynamics collects the metrics that are specific and useful to your organization, and those metrics can contribute to current business operations before and after a migration.

### Example:

A company that sells widgets from an online marketplace has identified the following key business transactions within their web application:

- Landing page
- Add to cart
- Shipping
- Billing
- Confirm order

These types of business transactions are common to e-commerce applications. A conversion funnel is the journey that a user takes through these pages, and it directly leads to sales revenue on the company's platform. When users abandon the journey because of poor page performance or errors, this directly impacts the company's underlying profit.

Additionally, the company has identified the following key business metrics:

- Cart totals
- Customer segments
- Customer locations

Combining application and business performance metrics helps to clearly demonstrate how their application's performance relates to their underlying profit. This level of visibility and types of insights will be vital during migrations.

Configurable dashboards are one of many AppDynamics tools that visualize these insights. In this real-time example, we see the overall conversion funnel and the impact on individual page performance against abandoners alongside shopping cart totals, customer segment, location, and general revenue details.

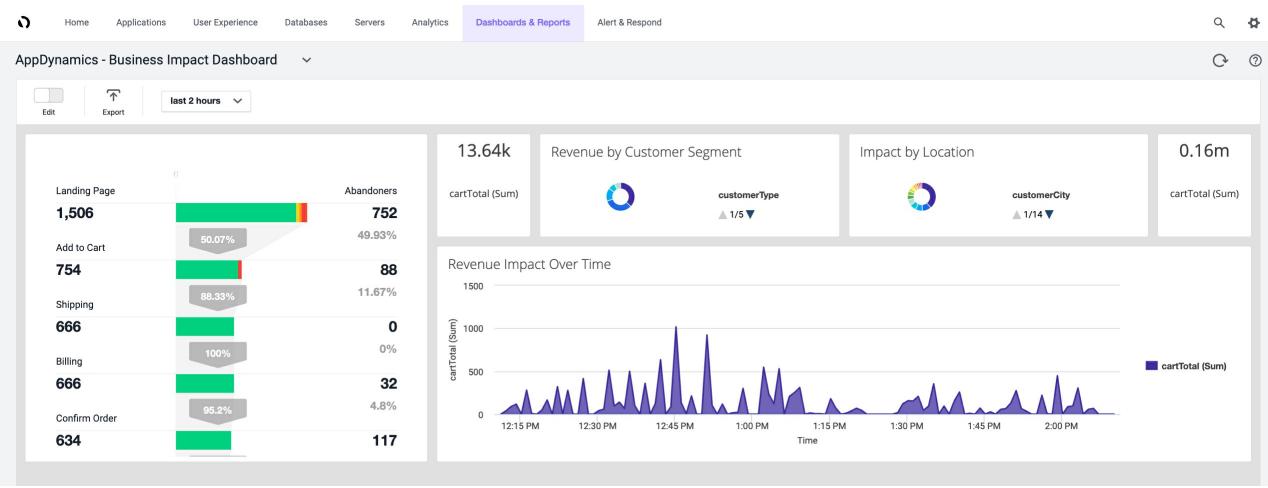


Figure 2: AppDynamics business impact dashboard.

## Resources to help identify business metrics

The [strategy](#) and [business outcomes](#) sections of the Cloud Adoption Framework provide the guidance and strategies to help you identify business outcomes for your organization.

## Pre- and post-migration comparison

The cloud offers vast benefits and potential, but the first steps of a migration are often unclear and full of risk. A successful migration must be evaluated by more criteria than the capability for a successful deployment.

Understanding the pre- and post-cloud-migration user experience and business performance helps you to adjust and stabilize both, when needed, which can help to produce successful business outcomes while reinforcing the value that Azure provides throughout your migration journey.

To build on the foundation of understanding how AppDynamics provides business and application metrics, compare those metrics before and after a migration to evaluate its success and if the target business outcomes are met.

### Example:

Movie Tickets Online, a fictitious online movie ticket seller, is working to retire their existing datacenters and move their workloads to Azure. Their capacity issues have led to poor business transaction performance, and they look forward to the performance optimizations and capacity in Azure.

In addition to improving performance, they want to ensure that the business outcomes of improving their sales funnels and growing their revenue will be met. As part of their migration, they deployed AppDynamics to their existing on-premises environments to clearly understand their current performance. As part of the cloud deployment, Movie Tickets Online can use AppDynamics native integration with Azure to understand post-migration performance and business outcomes.

In this case, they were able to see an increase in conversion rates from 48 to 79 percent and improvements to underlying performance, response time, and ticket sales volume.

## PRE AND POST CLOUD MIGRATION

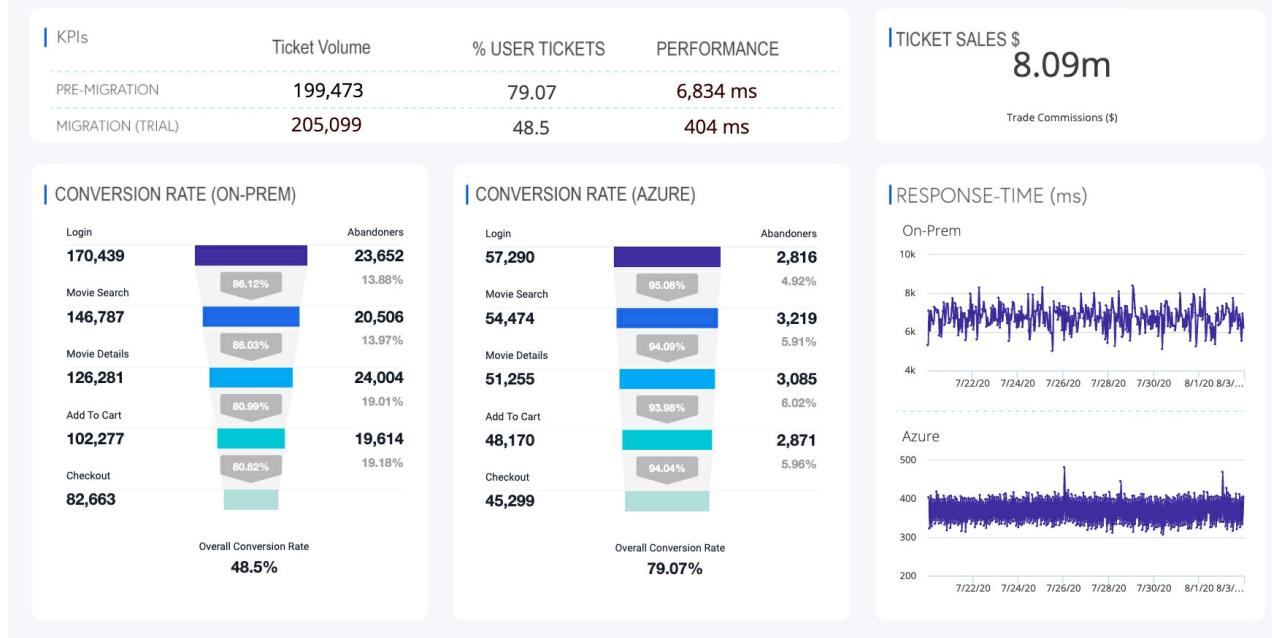


Figure 3: AppDynamics migration comparison.

## Next steps

AppDynamics gives organizations the unique ability to measure the business outcomes during their cloud adoption strategy. Visit [AppDynamics](#) to learn more about AppDynamics with Azure.

# Initial organization alignment

11/9/2020 • 2 minutes to read • [Edit Online](#)

The most important aspect of any cloud adoption plan is the alignment of people who will make the plan a reality. No plan is complete until you understand its people-related aspects.

True organizational alignment takes time. It will become important to establish long-term organizational alignment, especially as cloud adoption scales across the business and IT culture. Alignment is so important that an entire section has been dedicated to it in the [Organize methodology](#) of the Cloud Adoption Framework.

Full organization alignment is not a required component of the cloud adoption plan. However, some initial organization alignment is needed. This article outlines a best-practice starting point for organizational alignment. The guidance here can help complete your plan and get your teams ready for cloud adoption. When you're ready, you can use the [organization alignment](#) section to customize this guidance to fit your organization.

## Initial best-practice structure

To create a balance between speed and control, we recommend that during cloud adoption, at a minimum, you have people accountable for *cloud adoption* and *cloud governance*. This might be a team of people sharing responsibilities for each of these areas, or *capabilities*. It might also be individual people who are both accountable for the outcomes and responsible for the work. In either scenario, cloud adoption and cloud governance are two capabilities that involve natural friction between moving quickly and reducing risks. Here's how the two teams fit together:



It's fairly intuitive that cloud adoption tasks require people to execute those tasks. So, few people are surprised that a cloud adoption team is a requirement. However, those who are new to the cloud may not fully appreciate the importance of a cloud governance team. This challenge often occurs early in adoption cycles. The cloud governance team provides the necessary checks and balances to ensure that cloud adoption doesn't expose the business to any new risks. When risks must be taken, this team ensures that proper processes and controls are implemented to mitigate or govern those risks.

For more information about cloud adoption, cloud governance, and other such capabilities, see the brief section on [understanding required cloud capabilities](#).

## Map people to capabilities

Assuming that the suggested structure aligns to your cloud adoption plan, the next step is to map specific people to the necessary capabilities. To do so, answer the following questions:

- What person (or group of people) will be responsible for completing technical tasks in the cloud adoption plan?
- What person will be accountable for the team's ability to deliver technical changes?
- What person (or group of people) will be responsible for implementing protective governance mechanisms?
- What person will be accountable for the defining those governance controls?
- Are there other capabilities or people that will have accountability or responsibility within the cloud adoption

plan?

After you've documented the answers to these questions, you can establish [plans for skills readiness](#) to define plans to prepare these people for forthcoming work.

## Next steps

Learn how to plan for cloud adoption.

[Plan for cloud adoption](#)

# Adapt existing roles, skills, and processes for the cloud

11/9/2020 • 3 minutes to read • [Edit Online](#)

At each phase of the IT industry's history, the most notable changes have often been marked by changes in staff roles. One example is the transition from mainframe computing to client/server computing. The role of the computer operator during this transition has largely disappeared, replaced by the system administrator role. When virtualization arrived, the requirement for individuals working with physical servers was replaced with a need for virtualization specialists.

Roles will likely change as institutions similarly shift to cloud computing. For example, datacenter specialists might be replaced with cloud administrators or cloud architects. In some cases, though IT job titles haven't changed, the daily work of these roles has changed significantly.

IT staff members might feel anxious about their roles and positions because they realize that they need a different set of skills to support cloud solutions. But agile employees who explore and learn new cloud technologies shouldn't fear. They can lead the adoption of cloud services and help the organization learn and embrace the associated changes.

For guidance on building a new skill set, see the [skills readiness path](#).

## Capture concerns

As the organization prepares for a cloud adoption effort, each team should document staff concerns as they arise by identifying:

- The type of concern. For example, workers might be resistant to the changes in job duties that come with the adoption effort.
- The impact if the concern isn't addressed. For example, resistance to adoption might result in workers being slow to execute the required changes.
- The area equipped to address the concern. For example, if workers in the IT department are reluctant to acquire new skills, the IT stakeholder's area is best equipped to address this concern. Identifying the area might be clear for some concerns. In these cases, you might need to escalate to executive leadership.

IT staff members commonly have concerns about acquiring the training needed to support expanded functions and new duties. Learning the training preferences of the team helps you prepare a plan. It also allows you to address these concerns.

## Identify gaps

Identifying gaps is another important aspect of organization readiness. A *gap* is a role, skill, or process that is required for your digital transformation but doesn't currently exist in your enterprise.

1. Enumerate the responsibilities that come with the digital transformation. Emphasize new responsibilities and existing responsibilities to be retired.
2. Identify the area that aligns with each responsibility. For each new responsibility, check how closely it aligns with the area. Some responsibilities might span several areas. This crossover represents an opportunity for better alignment that you should document as a concern. In the case where no area is identified as being responsible, document this gap.
3. Identify the skills necessary to support each responsibility, and check if your enterprise has existing resources

with those skills. Where there are no existing resources, determine the training programs or talent acquisition necessary to fill the gaps. Also determine the deadline by which you must support each responsibility to keep your digital transformation on schedule.

4. Identify the roles that will execute these skills. Some of your existing workforce will assume parts of the roles. In other cases, entirely new roles might be necessary.

## Partner across teams

The skills necessary to fill the gaps in your organization's digital transformation are typically not confined to a single role or even a single department. Skills will have relationships and dependencies that can span a single role or multiple roles. Those roles might exist in several departments. For example, a workload owner might require someone in an IT role to provision core resources like subscriptions and resource groups.

These dependencies represent new processes that your organization implements to manage the workflow among roles. The preceding example shows several types of processes that support the relationship between the workload owner and the IT role. For instance, you can create a workflow tool to manage the process or use an email template.

Track these dependencies and make note of the processes that will support them. Also note whether the processes currently exist. For processes that require tooling, ensure that the timeline for deploying any tools aligns with the overall digital-transformation schedule.

## Next steps

Ensuring proper support for the translated roles is a team effort. To act on this guidance, review the organizational readiness overview to identify the right team structures and participants.

### [Identify the right team structures](#)

# Get started on a skills readiness path

11/9/2020 • 2 minutes to read • [Edit Online](#)

IT staff members might feel anxious about their roles and positions as they realize a different set of skills is needed to support cloud solutions. Agile employees who explore and learn new cloud technologies don't need to have that fear. They can lead the adoption of cloud services by helping the organization understand and embrace the associated changes.

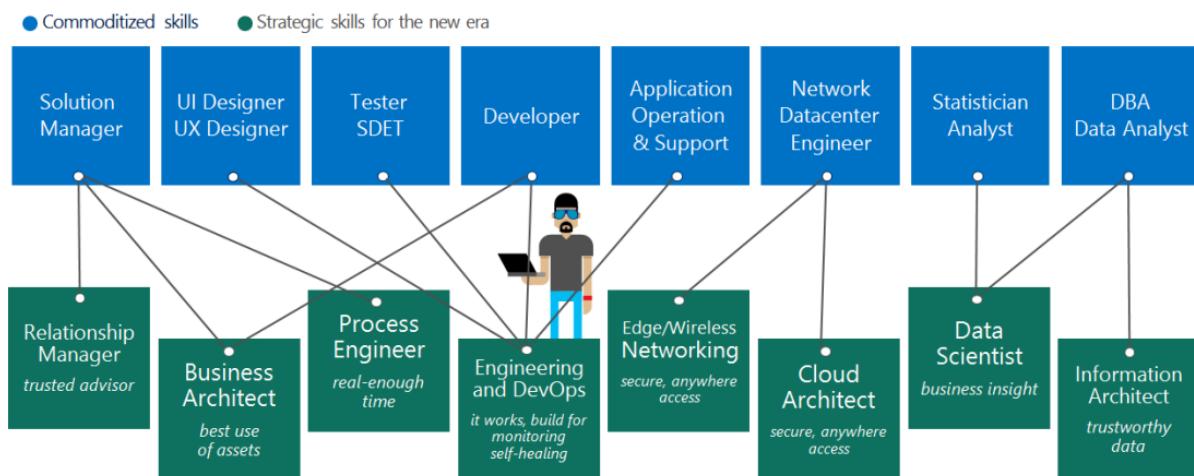


Figure 1: Mapping of skills to IT roles in a cloud-hosted environment.

The Cloud Adoption Framework guides readers through the full adoption lifecycle. Throughout this framework, readers are provided opportunities to build necessary skills. To help you get started on this journey, skills-readiness articles are included in the following outline for easier access. Each of the following links maps to the skills required to be successful in each of those adoption phases.

- **Strategy:** Develop the skills needed to prepare an actionable migration plan. This includes business justification and other required business-planning skills.
- **Plan:** Develop the skills needed to prepare an actionable migration plan. This includes business justification and other required business-planning skills.
- **Ready:** Develop the skills needed to prepare the business, culture, people, and environment for coming changes.
- **Adopt:** Adoption skills are aligned to various technical efforts:
  - **Migrate:** Gain the skills required to implement the cloud migration plan.
  - **Innovate:** Gain the skills needed to deliver innovative new solutions.
- **Operate:** Skills related to the operating model for cloud adoption are aligned to various opportunities to gain skills:
  - **Govern:** Gain the skills needed to govern the cloud environment.
  - **Manage:** Gain the skills needed to manage a cloud environment.
  - **Monitor:** Gain the skills needed to monitor a cloud environment.

Each of the previous learning paths shares opportunities across multiple media types to maximize knowledge acquisition.

# Microsoft Learn

Microsoft Learn is a new approach to learning. Readiness for the new skills and responsibilities that come with cloud adoption doesn't come easily. Microsoft Learn provides a more rewarding approach to hands-on learning that helps you achieve your goals faster. Earn points and levels, and achieve more! Here are a couple examples of tailored learning paths on Microsoft Learn which align to the Plan methodology of the Cloud Adoption Framework:

**Evolve your DevOps practices:** DevOps is the union of people, process, and products to enable continuous delivery of value to your end users. Azure DevOps is a set of services that gives you the tools you need to do just that. With Azure DevOps, you can build, test, and deploy any application, either in the cloud or on premises.

**Azure for the data engineer:** Explore how the world of data has evolved and how the advent of cloud technologies is providing new opportunities for business to explore. You will learn the various data platform technologies that are available, and how a data engineer can take advantage of this technology to an organization's benefit.

## Learn more

To discover additional learning paths, browse the [Microsoft Learn catalog](#). Use the roles filter to align learning paths with your role.

# Plan for cloud adoption

5/12/2020 • 2 minutes to read • [Edit Online](#)

A plan is an essential requirement for a successful cloud adoption. A cloud adoption plan is an iterative project plan that helps a company transition from traditional IT approaches to transformation over to modern, agile approaches. This article series outlines how a cloud adoption plan helps companies balance their IT portfolio and manage transitions over time. Through this process, business objectives can be clearly translated into tangible technical efforts. Those efforts can then be managed and communicated in ways that make sense to business stakeholders. However, adopting such a process may require some changes to traditional project-management approaches.

## Align strategy and planning

Cloud adoption plans start with a well-defined strategy. At a minimum, the strategy should outline the motivations, business outcomes, and business justifications for cloud adoption. Those positive returns are then balanced by the effort required to realize them.

The effort starts with the digital estate (proposed or existing), which translates the strategy into more tangible workloads and assets. You can then map these tangible elements to technical work. From there, skilled people in a proper organizational structure can execute the technical work. The cloud adoption plan combines these topics into one plan that can be forecasted, budgeted, implemented, and managed by means of agile project-management practices. This article series helps you build the plan and provides a few templates to make the job easier.

## Transition from sequential to iterative planning

Planning for cloud adoption can be a significant change for some organizations. IT organizations have long focused on the application of linear or sequential models of project management, like the [waterfall model](#). In traditional IT, this approach was entirely logical. Most large IT projects started with a procurement request to acquire expensive hardware resources. Capital expense requests, budget allocations, and equipment acquisition often represented a large percentage of project execution. And after it was acquired, the hardware itself became a constraint on what could be delivered.

The acquisition models of the cloud change the core dependencies that made a sequential model necessary. The replacement of acquisition cycles with an operating-expense approach helps businesses move more quickly and with smaller financial commitments. This approach helps teams to engage in projects before all requirements are well known. It also creates room for a growth mindset, which frees the team to experiment, learn, and deliver without artificial constraints. For all these reasons and more, we highly recommend that teams use agile or iterative approaches to cloud adoption planning.

## Build your cloud adoption plan

This article series walks through each step of translating strategy and effort into an actionable cloud adoption plan:

1. **Prerequisites:** Confirm that all prerequisite steps have been completed before you create your plan.
2. **Define and prioritize workloads:** Prioritize your first 10 workloads to establish an initial adoption backlog.
3. **Align assets to workloads:** Identify which assets (proposed or existing) are required to support the prioritized workloads.
4. **Review rationalization decisions:** Review rationalization decisions to refine adoption path decisions:

migrate or innovate.

5. **Establish iterations and release plans:** *Iterations* are the time blocks allocated to do work. *Releases* are the definition of the work to be done before triggering a change to production processes.
6. **Estimate timelines:** Establish rough timelines for release planning purposes, based on initial estimates.

## Next steps

Before building your cloud adoption plan, ensure that all [necessary prerequisites](#) are in place.

[Review prerequisites](#)

# Prerequisites for an effective cloud adoption plan

11/9/2020 • 2 minutes to read • [Edit Online](#)

A plan is only as effective as the data that's put into it. For a cloud adoption plan to be effective, there are two categories of input: *strategic* and *tactical*. The following sections outline the minimum data points required in each category.

## Strategic inputs

Accurate strategic inputs ensure that the work being done contributes to achievement of business outcomes. The [strategy section of the Cloud Adoption Framework](#) provides a series of exercises to develop a clear strategy. The outputs of those exercises feed the cloud adoption plan. Before developing the plan, ensure that the following items are well defined as a result of those exercises:

- **Clear motivations:** Why are we adopting the cloud?
- **Defined business outcomes:** What results do we expect to see from adopting the cloud?
- **Business justification:** How will the business measure success?

Every member of the team that implements the cloud adoption plan should be able to answer these three strategic questions. Managers and leaders who are accountable for implementation of the plan should understand the metrics behind each question and any progress toward realizing those metrics.

## Tactical inputs

Accurate tactical inputs ensure that the work can be planned accurately and managed effectively. The [plan section of the Cloud Adoption Framework](#) provides a series of exercises to develop planning artifacts before you develop your plan. These artifacts provide answers to the following questions:

- **Digital estate rationalization:** What are the top 10 priority workloads in the adoption plan? How many additional workloads are likely to be in the plan? How many assets are being considered as candidates for cloud adoption? Are the initial efforts focused more on migration or innovation activities?
- **Organization alignment:** Who will do the technical work in the adoption plan? Who is accountable for adherence to governance and compliance requirements?
- **Skills readiness:** How many people are allocated to perform the required tasks? How well are their skills aligned to cloud adoption efforts? Are partners aligned to support the technical implementation?

These questions are essential to the accuracy of the cloud adoption plan. At a minimum, the questions about digital estate rationalization must be answered to create a plan. To provide accurate timelines, the questions about organization and skills are also important.

## Next steps

Define your cloud adoption plan by deploying the template to Azure DevOps Services.

[Define your cloud adoption plan using the template](#)

# Cloud adoption plan and Azure DevOps

11/9/2020 • 3 minutes to read • [Edit Online](#)

Azure DevOps is the set of cloud-based tools for Azure customers who manage iterative projects. It also includes tools for managing deployment pipelines and other important aspects of DevOps.

In this article, you'll learn how to quickly deploy a backlog to Azure DevOps using a template. This template aligns cloud adoption efforts to a standardized process based on the guidance in the Cloud Adoption Framework.

## Create your cloud adoption plan

To deploy the cloud adoption plan, open the [Azure DevOps demo generator](#). This tool will deploy the template to your Azure DevOps tenant. Using the tool requires the following steps:

1. Verify that the **Selected Template** field is set to **Cloud Adoption Plan**. If it isn't, select **Choose template** to choose the right template.
2. Select your Azure DevOps organization from the **Select Organization** drop-down list box.
3. Enter a name for your new project. The cloud adoption plan will have this name when it's deployed to your Azure DevOps tenant.
4. Select **Create Project** to create a new project in your tenant, based on the strategy and plan template. A progress bar show your progress toward deploying the project.
5. When deployment is finished, select **Navigate to project** to see your new project.

After your project has been created, continue through this article series to learn how to modify the template to align to your cloud adoption plan.

For additional support and guidance on this tool, see [Azure DevOps Services demo generator](#).

## Bulk edit the cloud adoption plan

When the plan project has been deployed, you can use Microsoft Excel to modify it. It's much easier to create new workloads or assets in the plan by using Microsoft Excel than by using the Azure DevOps browser experience.

To prepare your workstation for bulk editing, see [Bulk add or modify work items with Microsoft Excel](#).

Some users may want to use Project to track their tasks, create backlog and assign resource. Here are the steps to [connect Project to Azure DevOps](#).

## Use the cloud adoption plan

The cloud adoption plan organizes activities by activity type:

- **Epic**: An *epic* represents an overall phase of the cloud adoption lifecycle.
- **Features**: Features are used to organize specific objectives within each phase. For instance, migration of a specific workload would be one feature.
- **User stories**: User stories group work into logical collections of activities based on a specific goal.
- **Tasks**: Tasks are the actual work to be done.

At each layer, activities are then sequenced based on dependencies. Activities are linked to articles in the Cloud Adoption Framework to clarify the objective or task at hand.

The clearest view of the cloud adoption plan comes from the **Epics backlog** view. For help with changing to the

Epic backlog view, see the article on [viewing a backlog](#). From this view, it's easy to plan and manage the work required to complete the current phase of the adoption lifecycle.

#### NOTE

The current state of the cloud adoption plan focuses heavily on migration efforts. Tasks related to governance, innovation, or operations must be populated manually.

## Align the cloud adoption plan

The overview pages for the Strategy methodology and the Plan methodology each refer to the [strategy and plan template](#). That template organizes the decisions and data points that will align the template for the cloud adoption plan with your specific plans for adoption. Considering completing the exercises in the [Strategy methodology](#) and the [Plan methodology](#) before aligning your new project.

The following articles support alignment of the cloud adoption plan:

- [Workloads](#): Align features within the cloud migration epic to capture each workload to be migrated or modernized. Add and modify those features to capture the effort to migrate your top 10 workloads.
- [Assets](#): Each asset (virtual machine, application, or data) is represented by the user stories under each workload. Add and modify those user stories to align with your digital estate.
- [Rationalization](#): As each workload is defined, the initial assumptions about that workload can be challenged. This might result in changes to the tasks under each asset.
- [Create release plans](#): Iteration paths establish release plans by aligning efforts with various releases and iterations.
- [Establish timelines](#): Defining start and end dates for each iteration creates a timeline to manage the overall project.

These five articles help with each of the alignment tasks required to start managing your adoption efforts. The next step gets you started on the alignment exercise.

## Next steps

Start aligning your plan project by [defining and prioritizing workloads](#).

[Define and prioritize workloads](#)

# Define and prioritize workloads for a cloud adoption plan

11/9/2020 • 5 minutes to read • [Edit Online](#)

Establishing clear, actionable priorities is one of the secrets to successful cloud adoption. The natural temptation is to invest time in defining all workloads that could potentially be affected during cloud adoption. But that's counterproductive, especially early in the adoption process.

Instead, we recommend that your team focus on thoroughly prioritizing and documenting the first 10 workloads. After implementation of the adoption plan begins, the team can maintain a list of the next 10 highest-priority workloads. This approach provides enough information to plan for the next few iterations.

Limiting the plan to 10 workloads encourages agility and alignment of priorities as business criteria change. This approach also makes room for the cloud adoption team to learn and to refine estimates. Most important, it removes extensive planning as a barrier to effective business change.

## What is a workload?

In the context of a cloud adoption, a workload is a collection of IT assets (servers, VMs, applications, data, or appliances) that collectively support a defined process. Workloads can support more than one process.

Workloads can also depend on other shared assets or larger platforms. However, a workload should have defined boundaries regarding the dependent assets and the processes that depend upon the workload. Often, workloads can be visualized by monitoring network traffic among IT assets.

## Prerequisites

The strategic inputs from the prerequisites list make the following tasks much easier to accomplish. For help with gathering the data discussed in this article, review the [prerequisites](#).

## Initial workload prioritization

During the process of [incremental rationalization](#), your team should agree on a [Power of 10 approach](#), consisting of 10 priority workloads. These workloads serve as an initial boundary for adoption planning.

If you decide that a digital estate rationalization isn't needed, we recommend that the cloud adoption teams and the cloud strategy team agree on a list of 10 applications to serve as the initial focus of the migration. We recommend further that these 10 workloads contain a mixture of simple workloads (fewer than 10 assets in a self-contained deployment) and more complex workloads. Those 10 workloads will start the workload prioritization process.

### NOTE

The Power of 10 approach serves as an initial boundary for planning, to focus the energy and investment in early-stage analysis. However, the act of analyzing and defining workloads is likely to cause changes in the list of priority workloads.

## Add workloads to your cloud adoption plan

In the previous article, [Cloud adoption plan and Azure DevOps](#), you created a cloud adoption plan in Azure DevOps.

You can now represent the workloads in the Power of 10 list in your cloud adoption plan. The easiest way to do this is via bulk editing in Microsoft Excel. To prepare your workstation for bulk editing, see [Bulk add or modify work items with Microsoft Excel](#).

Step 5 in that article tells you to select **Input list**. Instead, select **Query list**. Then, from the **Select a Query** drop-down list, select the **Workload Template** query. That query loads all the efforts related to the migration of a single workload into your spreadsheet.

After the work items for the workload template are loaded, follow these steps to begin adding new workloads:

1. Copy all the items that have the **Workload Template** tag in the far right column.
2. Paste the copied rows below the last line item in the table.
3. Change the title cell for the new feature from **Workload Template** to the name of your new workload.
4. Paste the new workload name cell into the tag column for all rows below the new feature. Be careful to not change the tags or name of the rows related to the actual **Workload Template** feature. You will need those work items when you add the next workload to the cloud adoption plan.
5. Skip to step 8 in the bulk-editing instructions to publish the worksheet. This step creates all the work items required to migrate your workload.

Repeat steps 1 through 5 for each of the workloads in the Power of 10 list.

## Define workloads

After initial priorities have been defined and workloads have been added to the plan, each of the workloads can be defined via deeper qualitative analysis. Before including any workload in the cloud adoption plan, try to provide the following data points for each workload.

### Business inputs

DATA POINT	DESCRIPTION	INPUT
Workload name	What is this workload called?	
Workload description	In one sentence, what does this workload do?	
Adoption motivations	Which of the cloud adoption motivations are affected by this workload?	
Primary sponsor	Of those stakeholders affected, who is the primary sponsor requesting the preceding motivations?	
Business impact	What is the business impact of this workload?	
Application impact	What impact does this application have on business processes?	
Data impact	What impact does the data have on the business?	
Business unit	Which business unit is responsible for the cost of this workload?	

DATA POINT	DESCRIPTION	INPUT
Business processes	Which business processes will be affected by changes to the workload?	
Business teams	Which business teams will be affected by changes?	
Business stakeholders	Are there any executives whose business will be affected by changes?	
Business outcomes	How will the business measure the success of this effort?	
Metrics	What metrics will be used to track success?	
Compliance	Are there any third-party compliance requirements for this workload?	
Application owners	Who is accountable for the business impact of any applications associated with this workload?	
Business freeze periods	Are there any times during which the business will not permit change?	
Geographies	Are any geographies affected by this workload?	

### Technical inputs

DATA POINT	DESCRIPTION	INPUT
Adoption approach	Is this adoption a candidate for migration or innovation?	
Application ops lead	List the parties responsible for performance and availability of this workload.	
SLAs	List any service-level agreements (RTO/RPO requirements).	
Criticality	List the current application criticality.	
Data classification	List the classification of data sensitivity.	
Operating geographies	List any geographies in which the workload is or should be hosted.	
Applications	Specify an initial list or count of any applications included in this workload.	

DATA POINT	DESCRIPTION	INPUT
VMs	Specify an initial list or count of any VMs or servers included in the workload.	
Data sources	Specify an initial list or count of any data sources included in the workload.	
Dependencies	List any asset dependencies not included in the workload.	
User traffic geographies	List geographies that have a significant collection of user traffic.	

## Confirm priorities

Based on the assembled data, the cloud strategy team and the cloud adoption team should meet to reevaluate priorities. Clarification of business data points might prompt changes in priorities. Technical complexity or dependencies might result in changes related to staffing allocations, timelines, or sequencing of technical efforts.

After a review, both teams should be comfortable with confirming the resulting priorities. This set of documented, validated, and confirmed priorities is the prioritized cloud adoption backlog.

## Next steps

For any workload in the prioritized cloud adoption backlog, the team is now ready to [align assets](#).

[Align assets for prioritized workloads](#)

# Align assets to prioritized workloads

11/9/2020 • 2 minutes to read • [Edit Online](#)

Workload is a conceptual description of a collection of assets: VMs, applications, and data sources. The previous article, [Define and prioritize](#), provided guidance for collecting the data that will define the workload. Before migration, a few of the technical inputs in that list require additional validation. This article helps with validation of the following inputs:

- **Applications:** List any applications included in this workload.
- **VMs and servers:** List any VMs or servers included in the workload.
- **Data sources:** List any data sources included in the workload.
- **Dependencies:** List any asset dependencies not included in the workload.

There are several options for assembling this data. The following are a few of the most common approaches.

## Alternative inputs: Migrate, modernize, innovate

The objective of the preceding data points is to capture relative technical effort and dependencies as an aid to prioritization. Depending on the transition you want, you may need to gather alternative data points to support proper prioritization.

**Migrate:** For pure migration efforts, the existing inventory and asset dependencies serve as a fair measure of relative complexity.

**Modernize:** When the goal for a workload is to modernize applications or other assets, these data points are still solid measures of complexity. However, it might be wise to add an input for modernization opportunities to the workload documentation.

**Innovate:** When data or business logic is undergoing material change during a cloud adoption effort, it's considered an *innovate* type of transformation. The same is true when you're creating new data or new business logic. For any innovate scenarios, the migration of assets will likely represent the smallest amount of effort required. For these scenarios, the team should devise a set of technical data inputs to measure relative complexity.

## Azure Migrate

Azure Migrate provides a set of grouping functions that can speed up the aggregation of applications, VMs, data sources, and dependencies. After workloads have been defined conceptually, they can be used as the basis for grouping assets based on dependency mapping.

The Azure Migrate documentation provides guidance on [how to group machines based on dependencies](#).

## Configuration-management database

Some organizations have a well-maintained configuration-management database (CMDB) within their existing operations-management tooling. They could use the CMDB alternatively to provide the input data points discussed earlier.

## Next steps

[Review rationalization decisions](#) based on asset alignment and workload definitions.

[Review rationalization decisions](#)



# Review rationalization decisions

11/9/2020 • 4 minutes to read • [Edit Online](#)

During initial strategy and planning stages, we suggest you apply an [incremental rationalization](#) approach to the digital estate. But this approach embeds some assumptions into the resulting decisions. We advise the cloud strategy team and the cloud adoption teams to review those decisions in light of expanded-workload documentation. This review is also a good time to involve business stakeholders and the executive sponsor in future state decisions.

## IMPORTANT

Further validation of the rationalization decisions will occur during the Assess phase of migration. This validation focuses on business review of the rationalization to align resources appropriately.

To validate rationalization decisions, use the following questions to facilitate a conversation with the business. The questions are grouped by the likely rationalization alignment.

## Innovation indicators

If the joint review of the following questions yields an affirmative answer, a workload might be a better candidate for innovation. Such a workload wouldn't be migrated via a lift and shift or modernize model. Instead, the business logic or data structures would be re-created as a new or rearchitected application. This approach can be more labor-intensive and time-consuming. But for a workload that represents significant business returns, the investment is justified.

- Do the applications in this workload create market differentiation?
- Is there a proposed or approved investment aimed at improving the experiences associated with the applications in this workload?
- Does the data in this workload make new product or service offerings available?
- Is there a proposed or approved investment aimed at taking advantage of the data associated with this workload?
- Can the effect of the market differentiation or new offerings be quantified? If so, does that return justify the increased cost of innovation during cloud adoption?

The following two questions can help you include high-level technical scenarios in the rationalization review. Answering "yes" to either could identify ways of accounting for or reducing the cost associated with innovation.

- Will the data structures or business logic change during the course of cloud adoption?
- Is an existing deployment pipeline used to deploy this workload to production?

If the answer to either question is "yes," the team should consider including this workload as an innovation candidate. At a minimum, the team should flag this workload for architecture review to identify modernization opportunities.

## Migration indicators

Migration is a faster and cheaper way of adopting the cloud. But it doesn't take advantage of opportunities to innovate. Before you invest in innovation, answer the following questions. They can help you determine if a migration model is more applicable for a workload.

- Is the source code supporting this application stable? Do you expect it to remain stable and unchanged during the time frame of this release cycle?
- Does this workload support production business processes today? Will it do so throughout the course of this release cycle?
- Is it a priority that this cloud adoption effort improves the stability and performance of this workload?
- Is cost reduction associated with this workload an objective during this effort?
- Is reducing operational complexity for this workload a goal during this effort?
- Is innovation limited by the current architecture or IT operation processes?

If the answer to any of these questions is "yes," you should consider a migration model for this workload. This recommendation is true even if the workload is a candidate for innovation.

Challenges in operational complexity, costs, performance, or stability can hinder business returns. You can use the cloud to quickly produce improvements related to those challenges. Where it's applicable, we suggest you use the migration approach to first stabilize the workload. Then expand on innovation opportunities in the stable, agile cloud environment. This approach provides short-term returns and reduces the cost required to drive long-term change.

#### **IMPORTANT**

Migration models include incremental modernization. Using platform as a service (PaaS) architectures is a common aspect of migration activities. So too are minor configuration changes that use those platform services. The boundary for migration is defined as a material change to the business logic or supporting business structures. Such change is considered an innovation effort.

## Update the project plan

The skills required for a migration effort are different from the skills required for an innovation effort. During implementation of a cloud adoption plan, we suggest that you assign migration and innovation efforts to different teams. Each team has its own iteration, release, and planning cadences. Assigning separate teams provides the process flexibility to maintain one cloud adoption plan while accounting for innovation and migration efforts.

When you manage the cloud adoption plan in Azure DevOps, that management is reflected by changing the parent work item (or epic) from cloud migration to cloud innovation. This subtle change helps ensure all participants in the cloud adoption plan can quickly track the required effort and changes to remediation efforts. This tracking also helps align proper assignments to the relevant cloud adoption team.

For large, complex adoption plans with multiple distinct projects, consider updating the iteration path. Changing the area path makes the workload visible only to the team assigned to that area path. This change can make work easier for the cloud adoption team by reducing the number of visible tasks. But it adds complexity for the project management processes.

## Next steps

[Establish iterations and release plans to begin planning work.](#)

[Establish iterations and release plans to begin planning work.](#)

# Establish iterations and release plans

3/31/2020 • 4 minutes to read • [Edit Online](#)

Agile and other iterative methodologies are built on the concepts of iterations and releases. This article outlines the assignment of iterations and releases during planning. Those assignments drive timeline visibility to make conversations easier among members of the cloud strategy team. The assignments also align technical tasks in a way that the cloud adoption team can manage during implementation.

## Establish iterations

In an iterative approach to technical implementation, you plan technical efforts around recurring time blocks. Iterations tend to be one-week to six-week time blocks. Consensus suggests that two weeks is the average iteration duration for most cloud adoption teams. But the choice of iteration duration depends on the type of technical effort, the administrative overhead, and the team's preference.

To begin aligning efforts to a timeline, we suggest that you define a set of iterations that last 6 to 12 months.

## Understand velocity

Aligning efforts to iterations and releases requires an understanding of velocity. Velocity is the amount of work that can be completed in any given iteration. During early planning, velocity is an estimate. After several iterations, velocity becomes a highly valuable indicator of the commitments that the team can make confidently.

You can measure velocity in abstract terms like story points. You can also measure it in more tangible terms like hours. For most iterative frameworks, we recommend using abstract measurements to avoid challenges in precision and perception. Examples in this article represent velocity in hours per sprint. This representation makes the topic more universally understood.

**Example:** A five-person cloud adoption team has committed to two-week sprints. Given current obligations like meetings and support of other processes, each team member can consistently contribute 20 hours per week to the adoption effort. For this team, the initial velocity estimate is 100 hours per sprint.

## Iteration planning

Initially, you plan iterations by evaluating the technical tasks based on the prioritized backlog. Cloud adoption teams estimate the effort required to complete various tasks. Those tasks are then assigned to the first available iteration.

During iteration planning, the cloud adoption teams validate and refine estimates. They do so until they have aligned all available velocity to specific tasks. This process continues for each prioritized workload until all efforts align to a forecasted iteration.

In this process, the team validates the tasks assigned to the next sprint. The team updates its estimates based on the team's conversation about each task. The team then adds each estimated task to the next sprint until the available velocity is met. Finally, the team estimates additional tasks and adds them to the next iteration. The team performs these steps until the velocity of that iteration is also exhausted.

The preceding process continues until all tasks are assigned to an iteration.

**Example:** Let's build on the previous example. Assume each workload migration requires 40 tasks. Also assume you estimate each task to take an average of one hour. The combined estimation is approximately 40 hours per workload migration. If these estimates remain consistent for all 10 of the prioritized workloads, those workloads

will take 400 hours.

The velocity defined in the previous example suggests that the migration of the first 10 workloads will take four iterations, which is two months of calendar time. The first iteration will consist of 100 tasks that result in the migration of two workloads. In the next iteration, a similar collection of 100 tasks will result in the migration of three workloads.

#### WARNING

The preceding numbers of tasks and estimates are strictly used as an example. Technical tasks are seldom that consistent. You shouldn't see this example as a reflection of the amount of time required to migrate a workload.

## Release planning

Within cloud adoption, a release is defined as a collection of deliverables that produce enough business value to justify the risk of disruption to business processes.

Releasing any workload-related changes into a production environment creates some changes to business processes. Ideally, these changes are seamless, and the business sees the value of the changes with no significant disruptions to service. But the risk of business disruption is present with any change and shouldn't be taken lightly.

To ensure a change is justified by its potential return, the cloud strategy team should participate in release planning. Once tasks are aligned to sprints, the team can determine a rough timeline of when each workload will be ready for production release. The cloud strategy team would review the timing of each release. The team would then identify the inflection point between risk and business value.

**Example:** Continuing the previous example, the cloud strategy team has reviewed the iteration plan. The review identified two release points. During the second iteration, a total of five workloads will be ready for migration. Those five workloads will provide significant business value and will trigger the first release. The next release will come two iterations later, when the next five workloads are ready for release.

## Assign iteration paths and tags

For customers who manage cloud adoption plans in Azure DevOps, the previous processes are reflected by assigning an iteration path to each task and user story. We also recommend tagging each workload with a specific release. That tagging and assignment feed the automatic population of timeline reports.

## Next steps

[Estimate timelines](#) to properly communicate expectations.

[Estimate timelines](#)

# Timelines in a cloud adoption plan

11/9/2020 • 2 minutes to read • [Edit Online](#)

In the previous article in this series, workloads and tasks were assigned to [releases and iterations](#). Those assignments feed the timeline estimates in this article.

Work breakdown structures are commonly used in sequential project-management tools. They represent how dependent tasks will be completed over time. Such structures work well when tasks are sequential in nature. The interdependencies in tasks found in cloud adoption make such structures difficult to manage. To fill this gap, you can estimate timelines based on iteration-path assignments by hiding complexity.

## Estimate timelines

To develop a timeline, start with releases. Those release objectives create a target date for any business impact. Iterations aid in aligning those releases with specific time durations.

If more granular milestones are required in the timeline, use iteration assignment to indicate milestones. To do this assignment, assume that the last instance of a workload-related task can serve as the final milestone. Teams also commonly tag the final task as a milestone.

For any level of granularity, use the last day of the iteration as the date for each milestone. This ties completion of workload adoption to a specific date. You can track the date in a spreadsheet or a sequential project-management tool like Microsoft Project.

## Delivery plans in Azure DevOps

If you're using Azure DevOps to manage your cloud adoption plan, consider using the [Microsoft Delivery Plans extension](#). This extension can quickly create a visual representation of the timeline that is based on iteration and release assignments.

# Assess on-premises workloads for migration to Azure

11/9/2020 • 21 minutes to read • [Edit Online](#)

This article shows how the fictional company Contoso assesses an on-premises app for migration to Azure. In the example scenario, Contoso's on-premises SmartHotel360 application currently runs on VMware. Contoso assesses the application VMs using the Azure Migrate service, and the SQL Server application database using Data Migration Assistant.

## Overview

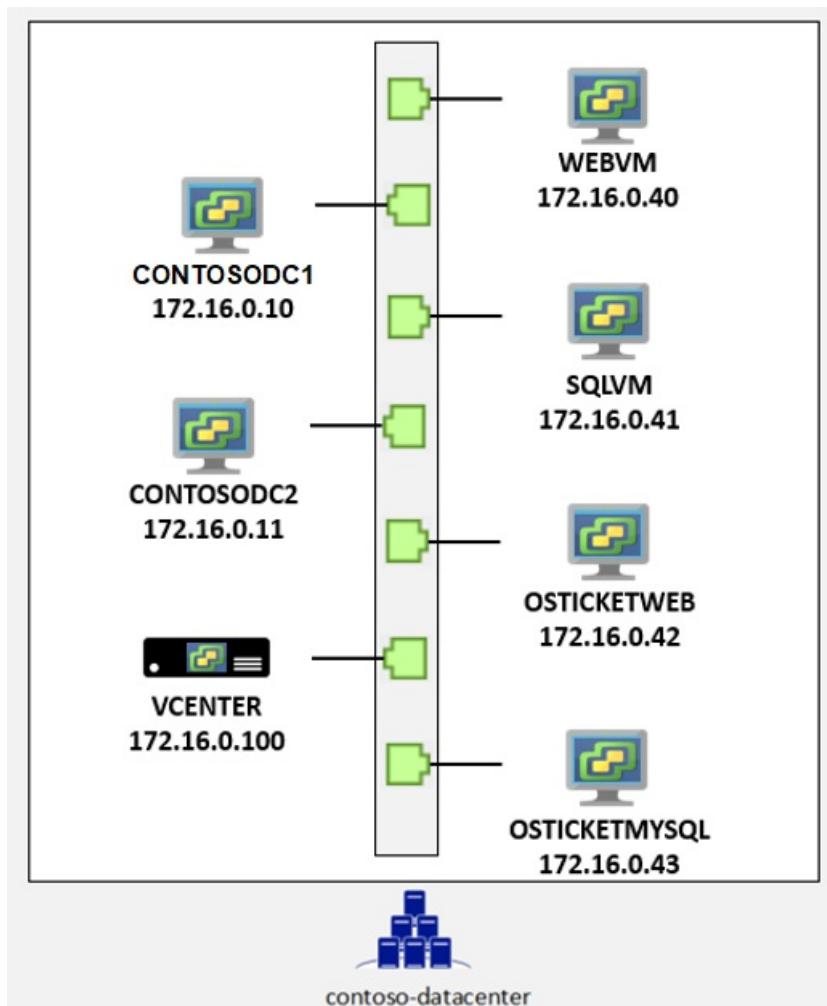
As Contoso considers migrating to Azure, the company needs a technical and financial assessment to determine whether its on-premises workloads are good candidates for cloud migration. In particular, the Contoso team wants to assess machine and database compatibility for migration. It wants to estimate capacity and costs for running Contoso's resources in Azure.

To get started and to better understand the technologies involved, Contoso assesses two of its on-premises apps, summarized in the following table. The company assesses for migration scenarios that rehost and refactor apps for migration. Learn more about rehosting and refactoring in the [migration examples overview](#).

APP NAME	PLATFORM	APP TIERS	DETAILS
SmartHotel360  (manages Contoso travel requirements)	Runs on Windows with a SQL Server database	Two-tiered app. The front-end ASP.NET website runs on one VM ( <code>WEBVM</code> ) and the SQL Server runs on another VM ( <code>SQLVM</code> ).	VMs run on a VMware ESXi host managed by vCenter Server.  You can download the sample app from <a href="#">GitHub</a> .
osTicket  (Contoso service desk app)	Runs on a LAMP stack.	Two-tiered app. A front-end PHP website runs on one VM ( <code>OSTICKETWEB</code> ) and the MySQL database runs on another VM ( <code>OSTICKETMYSQL</code> ).	The app is used by customer service apps to track issues for internal employees and external customers.  You can download the sample from <a href="#">GitHub</a> .

## Current architecture

This diagram shows the current Contoso on-premises infrastructure:



- Contoso has one main datacenter. The datacenter is located in the city of New York in the Eastern United States.
- Contoso has three additional local branches across the United States.
- The main datacenter is connected to the internet with a fiber optic Metro Ethernet connection (500 MBps).
- Each branch is connected locally to the internet by using business-class connections with IPsec VPN tunnels back to the main datacenter. The setup allows Contoso's entire network to be permanently connected and optimizes internet connectivity.
- The main datacenter is fully virtualized with VMware. Contoso has two ESXi 6.5 virtualization hosts that are managed by vCenter Server 6.5.
- Contoso uses Active Directory for identity management. Contoso uses DNS servers on the internal network.
- The domain controllers in the datacenter run on VMware VMs. The domain controllers at local branches run on physical servers.

## Business drivers

Contoso's IT leadership team has worked closely with the company's business partners to understand what the business wants to achieve with this migration:

- Address business growth.** Contoso is growing. As a result, pressure has increased on the company's on-premises systems and infrastructure.
- Increase efficiency.** Contoso needs to remove unnecessary procedures and streamline processes for its developers and users. The business needs IT to be fast and to not waste time or money, so the company can deliver faster on customer requirements.
- Increase agility.** Contoso IT needs to be more responsive to the needs of the business. It must be able to react faster than the changes that occur in the marketplace for the company to be successful in a global economy. IT at Contoso must not get in the way or become a business blocker.

- **Scale.** As the company's business grows successfully, Contoso IT must provide systems that can grow at the same pace.

## Assessment goals

The Contoso cloud team has identified goals for its migration assessments:

- After migration, apps in Azure should have the same performance capabilities that apps have today in Contoso's on-premises VMware environment. Moving to the cloud doesn't mean that app performance is less critical.
- Contoso needs to understand the compatibility of its applications and databases with Azure requirements. Contoso also needs to understand its hosting options in Azure.
- Contoso's database administration should be minimized after apps move to the cloud.
- Contoso wants to understand not only its migration options, but also the costs associated with the infrastructure after it moves to the cloud.

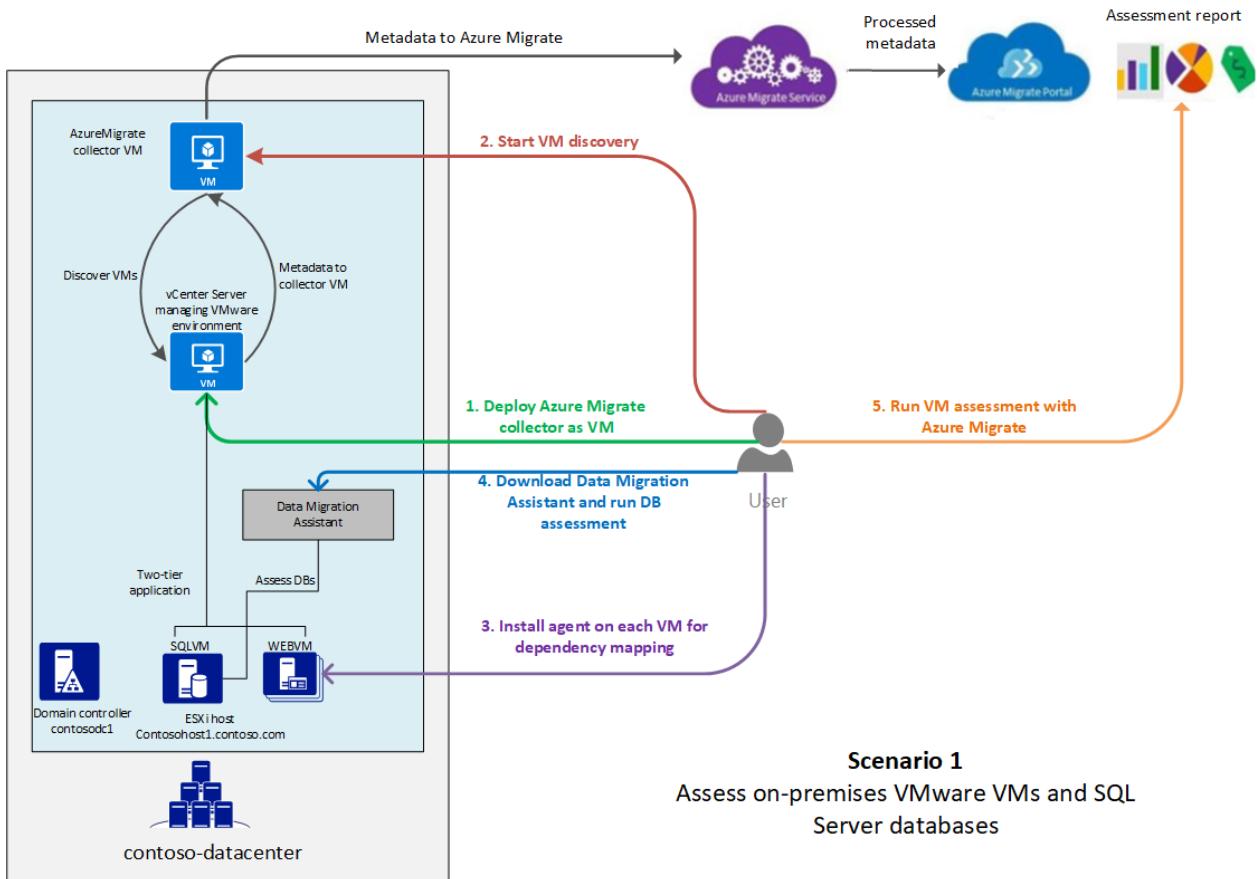
## Assessment tools

Contoso uses Microsoft tools for its migration assessment. The tools align with the company's goals and should provide Contoso with all the information it needs.

TECHNOLOGY	DESCRIPTION	COST
<a href="#">Data Migration Assistant</a>	Contoso uses Data Migration Assistant to assess and detect compatibility issues that might affect its database functionality in Azure. Data Migration Assistant assesses feature parity between SQL sources and targets. It recommends performance and reliability improvements.	Data Migration Assistant is a free downloadable tool.
<a href="#">Azure Migrate</a>	Contoso uses the Azure Migrate service to assess its VMware VMs. Azure Migrate assesses the migration suitability of the machines. It provides sizing and cost estimates for running in Azure.	Azure Migrate is available at no additional charge. However, you may incur charges depending on the tools (first-party or ISV) you decide to use for assessment and migration. Learn more about <a href="#">Azure Migrate pricing</a> .
<a href="#">Service Map</a>	Azure Migrate uses Service Map to show dependencies between machines that the company wants to migrate.	Service Map is part of Azure Monitor logs. Currently, Contoso can use Service Map for 180 days without incurring charges.

In this scenario, Contoso downloads and runs Data Migration Assistant to assess the on-premises SQL Server database for its travel app. Contoso uses Azure Migrate with dependency mapping to assess the app VMs before migration to Azure.

## Assessment architecture



- Contoso is a fictional name that represents a typical enterprise organization.
- Contoso has an on-premises datacenter ( `contoso-datacenter` ) and on-premises domain controllers ( `CONTOSODC1` , `CONTOSODC2` ).
- VMware VMs are located on VMware ESXi hosts running version 6.5 ( `contosohost1` , `contosohost2` ).
- The VMware environment is managed by vCenter Server 6.5 ( `vcenter.contoso.com` , running on a VM).
- The SmartHotel360 travel app has these characteristics:
  - The app is tiered across two VMware VMs ( `WEBVM` and `SQLVM` ).
  - The VMs are located on VMware ESXi host `contosohost1.contoso.com` .
  - The VMs are running Windows Server 2008 R2 Datacenter with SP1.
- The VMware environment is managed by vCenter Server ( `vcenter.contoso.com` ) running on a VM.
- The osTicket service desk app:
  - The app is tiered across two VMs ( `OSTICKETWEB` and `OSTICKETMYSQL` ).
  - The VMs are running Ubuntu Linux Server 16.04-LTS.
  - `OSTICKETWEB` is running Apache 2 and PHP 7.0.
  - `OSTICKETMYSQL` is running MySQL 5.7.22.

## Prerequisites

Contoso and other users must meet the following prerequisites for the assessment:

- Owner or Contributor permissions for the Azure subscription, or for a resource group in the Azure subscription.
- An on-premises vCenter Server instance running version 6.5, 6.0, or 5.5.
- A read-only account in vCenter Server, or permissions to create one.
- Permissions to create a VM on the vCenter Server instance by using an .ova template.
- At least one ESXi host running version 5.5 or later.

- At least two on-premises VMware VMs, one running a SQL Server database.
- Permissions to install Azure Migrate agents on each VM.
- The VMs should have direct internet connectivity.
  - You can restrict internet access to the [required URLs](#).
  - If your VMs don't have internet connectivity, the Azure [Log Analytics Gateway](#) must be installed on them, and agent traffic directed through it.
- The fully qualified domain name (FQDN) of the VM running the SQL Server instance, for database assessment.
- Windows Firewall running on the SQL Server VM should allow external connections on TCP port 1433 (default). This setup allows Data Migration Assistant to connect.

## Assessment overview

Here's how Contoso performs its assessment:

- **Step 1: Download and install Data Migration Assistant.** Contoso prepares Data Migration Assistant for assessment of the on-premises SQL Server database.
- **Step 2: Assess the database by using Data Migration Assistant.** Contoso runs and analyzes the database assessment.
- **Step 3: Prepare for VM assessment by using Azure Migrate.** Contoso sets up on-premises accounts and adjusts VMware settings.
- **Step 4: Discover on-premises VMs by using Azure Migrate.** Contoso creates an Azure Migrate collector VM. Then, Contoso runs the collector to discover VMs for assessment.
- **Step 5: Prepare for dependency analysis by using Azure Migrate.** Contoso installs Azure Migrate agents on the VMs, so the company can see dependency mapping between VMs.
- **Step 6: Assess the VMs by using Azure Migrate.** Contoso checks dependencies, groups the VMs, and runs the assessment. When the assessment is ready, Contoso analyzes the assessment in preparation for migration.

### NOTE

Assessments shouldn't just be limited to using tooling to discover information about your environment. You should also schedule time to speak to business owners, end users, and other members of the IT department to fully understand of what is happening in the environment and understand factors that tooling cannot tell you.

## Step 1: Download and install Data Migration Assistant

1. Contoso downloads Data Migration Assistant from the [Microsoft Download Center](#).
  - Data Migration Assistant can be installed on any machine that can connect to the SQL Server instance. Contoso doesn't need to run it on the SQL Server machine.
  - Data Migration Assistant shouldn't be run on the SQL Server host machine.
2. Contoso runs the downloaded setup file (DownloadMigrationAssistant.msi) to begin the installation.
3. On the **Finish** page, Contoso selects **Launch Microsoft Data Migration Assistant** before finishing the wizard.

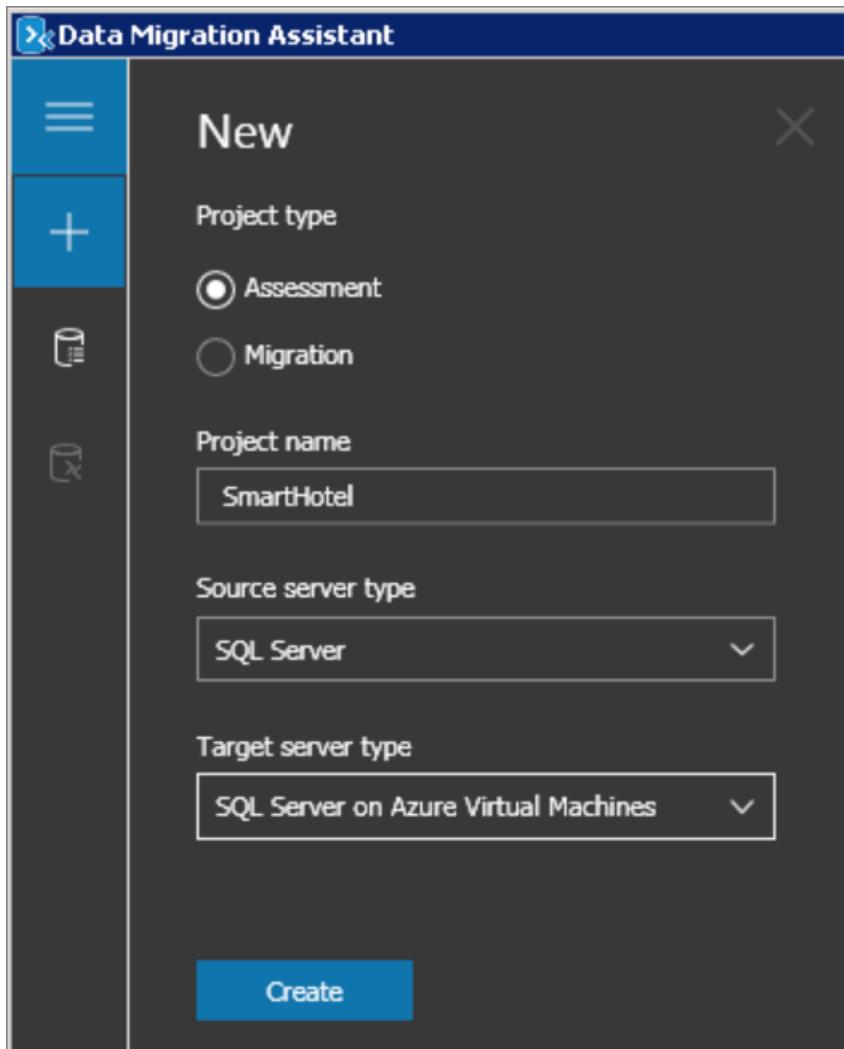
## Step 2: Run and analyze the database assessment for SmartHotel360

Now, Contoso can run an assessment to analyze its on-premises SQL Server database for the SmartHotel360 app.

1. In Data Migration Assistant, Contoso selects **New > Assessment**, and then gives the assessment a project

name.

2. For **Source server type**, Contoso selects SQL Server and for **Target Server type**, Contoso selects SQL Server on Azure Virtual Machines



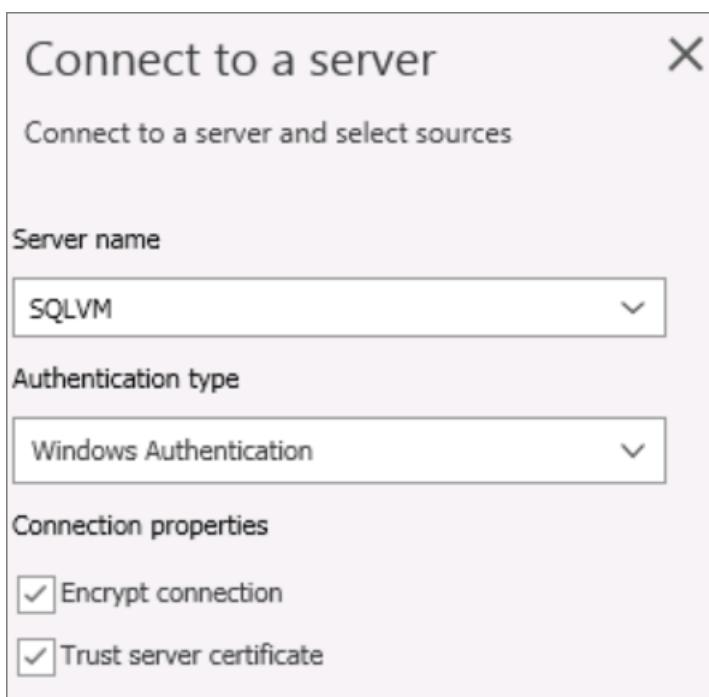
**NOTE**

Currently, Data Migration Assistant doesn't support assessment for migrating to Azure SQL Managed Instance. As a workaround, Contoso uses SQL Server on an Azure VM as the supposed target for the assessment.

3. In **Select Target Version**, Contoso selects SQL Server 2017 as the target version. Contoso needs to select this version because it's the version that's used by the SQL Managed Instance.
4. Contoso selects reports to help it discover information about compatibility and new features:
  - **Compatibility issues** note changes that might break migration or that require a minor adjustment before migration. This report keeps Contoso informed about any features currently in use that are deprecated. Issues are organized by compatibility level.
  - **New feature recommendation** notes new features in the target SQL Server platform that can be used for the database after migration. New feature recommendations are organized under the headings **Performance**, **Security**, and **Storage**.

The screenshot shows the 'Data Migration Assistant' interface for the 'SmartHotel' project. The top navigation bar includes 'Data Migration Assistant', a back arrow, the project name 'SmartHotel', and three tabs: '1 Options' (selected), '2 Select sources', and '3 Review results'. On the left, there's a sidebar with icons for 'Add source', 'Remove source', and 'Review results'. The main content area starts with 'Select target version' (set to 'SQL Server 2017 on Windows') and 'Select report type'. Three options are listed: 'Compatibility Issues' (checked, description: 'Discover breaking changes, behavior changes, and deprecated features by analyzing the databases you chose in your source server to be migrated to a new SQL Server platform.'), 'New features' recommendation' (checked, description: 'Discover new SQL Server features that are applicable to the databases and tables in your source server once migrated to the new target SQL Server platform.'), and 'Check feature parity' (unchecked, description: 'Discover unsupported or partially-supported features and functions that your applications may rely on. Get guidance around these areas that may need some re-engineering.').

5. In **Connect to a server**, Contoso enters the name of the VM that's running the database and credentials to access it. Contoso selects **Trust server certificate** to make sure the VM can access SQL Server. Then, Contoso selects **Connect**.



6. In **Add source**, Contoso adds the database it wants to assess, then selects **Next** to start the assessment.
7. The assessment is created.

The screenshot shows the 'Data Migration Assistant' interface for the 'SmartHotel' project, now at the '2 Select sources' step. The top navigation bar shows '1 Options' with a checkmark, '2 Select sources' (selected), and '3 Review results'. The sidebar icons are 'Add sources' (highlighted in blue) and 'Remove sources'. The main content area shows a table of databases under 'SQLVM (SQL Server 2008 R2) (1)'. The table has columns: Name, Compatibility Level, and Database Size. One row is visible: 'SmartHotel.Registration' with a compatibility level of 100 and a size of 2.74 MB.

8. In **Review results**, Contoso views the assessment results.

#### Analyze the database assessment

Results are displayed as soon as they're available. If Contoso fixes issues, it must select **Restart assessment** to

rerun the assessment.

1. In the **Compatibility issues** report, Contoso checks for any issues at each compatibility level.

Compatibility levels map to SQL Server versions as follows:

- 100: SQL Server 2008/Azure SQL Database
- 110: SQL Server 2012/Azure SQL Database
- 120: SQL Server 2014/Azure SQL Database
- 130: SQL Server 2016/Azure SQL Database
- 140: SQL Server 2017/Azure SQL Database

The screenshot shows the Data Migration Assistant interface. The left sidebar shows a tree view with 'SmartHotel' selected. The main pane is titled '3 Review results'. It displays the target platform as 'SQL Server 2017 on Windows'. Below that, it shows the database 'SmartHotel.Registration' with its properties: SQL Server 2008 R2, Compat 100, Size 2.74 MB. A table shows compatibility levels: Compatibility 120 (0), Compatibility 110 (0), Compatibility 100 (0), Compatibility 140 (0) (highlighted in green), and Compatibility 130 (0). A message box at the bottom right says ':-) There are no compatibility issues with your database.'

2. In the **Feature recommendations** report, Contoso views performance, security, and storage features that the assessment recommends after migration. A variety of features are recommended, including In-Memory OLTP, columnstore indexes, Stretch Database, Always Encrypted, dynamic data masking, and transparent data encryption.

The screenshot shows the Data Migration Assistant interface. The left sidebar shows a tree view with 'SmartHotel' selected. The main pane is titled '3 Review results'. It displays the target platform as 'SQL Server 2017 on Windows'. Below that, it shows the database 'SmartHotel.Registration' with its properties: SQL Server 2008 R2, Compat 100, Size 2.74 MB. A table shows feature recommendations: Performance (0), Security (2), and Storage (0). The 'Security' tab is selected, showing 2 medium-value recommendations: 'Security Advisor AE and DDM' and 'Security Advisor TDE'. The 'Security Advisor TDE' recommendation is expanded, showing its details: Impact (SQL Server 2016 improves performance of TDE by up to 70% through hardware acceleration), Objects (Database: SmartHotel.Registration), and Object details (Type: Database, Name: SmartHotel.Registration).

#### NOTE

Contoso should [enable transparent data encryption](#) for all SQL Server databases. This is even more critical when a database is in the cloud than when it's hosted on-premises. Transparent data encryption should be enabled only after migration. If transparent data encryption is already enabled, Contoso must move the certificate or asymmetric key to the `master` database of the target server. Learn how to [move a transparent data encryption-protected database to another SQL Server instance](#).

3. Contoso can export the assessment in JSON or CSV format.

#### NOTE

For large-scale assessments:

- Run multiple assessments concurrently and view the state of the assessments on the [All assessments](#) page.
- Consolidate assessments into a [SQL Server database](#).
- Consolidate assessments into a [Power BI report](#).

## Step 3: Prepare for VM assessment by using Azure Migrate

Contoso needs to create a VMware account that Azure Migrate can use to automatically discover VMs for assessment, verify rights to create a VM, note the ports that need to be opened, and set the statistics settings level.

### Set up a VMware account

VM discovery requires a read-only account in vCenter Server that has the following properties:

- **User type:** At least a read-only user.
- **Permissions:** For the datacenter object, select the **Propagate to Child Objects** checkbox. For **Role**, select **Read-only**.
- **Details:** The user is assigned at the datacenter level, with access to all objects in the datacenter.
- To restrict access, assign the **No access** role with the **Propagate to child** object to the child objects (vSphere hosts, data stores, VMs, and networks).

### Verify permissions to create a VM

Contoso verifies that it has permissions to create a VM by importing a file in .ova format. Learn how to [create and assign a role with privileges](#).

### Verify ports

The Contoso assessment uses dependency mapping. Dependency mapping requires an agent to be installed on VMs that will be assessed. The agent must be able to connect to Azure from TCP port 443 on each VM. Learn about [connection requirements](#).

## Step 4: Discover VMs

To discover VMs, Contoso creates an Azure Migrate project. Contoso downloads and sets up the collector VM. Then, Contoso runs the collector to discover its on-premises VMs.

### Create a project

Set up a new Azure Migrate project as follows.

1. In the Azure portal > All services, search for **Azure Migrate**.
2. Under **Services**, select **Azure Migrate**.
3. In **Overview**, under **Discover, assess and migrate servers**, select **Assess and migrate servers**.

4. In **Getting started**, select **Add tools**.
5. In **Migrate project**, select your Azure subscription, and create a resource group if you don't have one.
6. In **Project Details**, specify the project name, and the geography in which you want to create the project. United States, Asia, Europe, Australia, United Kingdom, Canada, India, and Japan are supported.
  - The project geography is used only to store the metadata gathered from on-premises VMs.
  - You can select any target region when you run a migration.
7. Select **Next**.
8. In **Select assessment tool**, select **Azure Migrate: Server Assessment > Next**.

TOOL	PRICING	SUPPORTED WORKLOADS	FEATURES	LEARN MORE
<b>Azure Migrate: Server Assessment</b>	<a href="#">View</a>	VMware virtual machines Hyper-V virtual machines	Agentless discovery Cost planning and optimal right sizing Application dependency analysis Cloud migration planning	<a href="#">Learn more</a>
<b>Cloudamize: Cloud Assessment</b>	<a href="#">View</a>	VMware virtual machines Hyper-V virtual machines Physical machines Workloads on other public clouds	Agentless or agent-based discovery Cost planning and optimal right sizing Application dependency analysis Cloud migration planning	<a href="#">Learn more</a>
<b>Corent Tech: SurPaaS MaaS</b>	<a href="#">View</a>	VMware virtual machines Hyper-V virtual machines Physical machines Workloads on other public clouds	Agentless or agent-based discovery Cost planning and optimal right sizing Application dependency analysis Cloud migration planning	<a href="#">Learn more</a>
<b>Turbonomic: Turbonomic</b>	<a href="#">View</a>	VMware virtual machines Hyper-V virtual machines Physical machines Workloads on other public clouds	Agentless discovery Cost planning and optimal right sizing Application dependency analysis Cloud migration planning	<a href="#">Learn more</a>
<b>UnifyCloud: CloudRecon</b>	<a href="#">View</a>	VMware virtual machines Hyper-V virtual machines Physical machines Workloads on other public clouds	Agentless or agent-based discovery Cost planning and optimal right sizing Application dependency analysis Cloud migration planning	<a href="#">Learn more</a>
<b>Device42: Device42</b>	<a href="#">View</a>	VMware virtual machines Hyper-V virtual machines Physical machines Workloads on other public clouds	Agentless discovery Cost planning and optimal right sizing Application dependency analysis Application workload grouping	<a href="#">Learn more</a>

Note: Visit the ISV tool's website to learn more about tool capabilities.  
Don't see a tool that you are looking for? We are continuously adding support for more ISV tools. [Learn more](#)

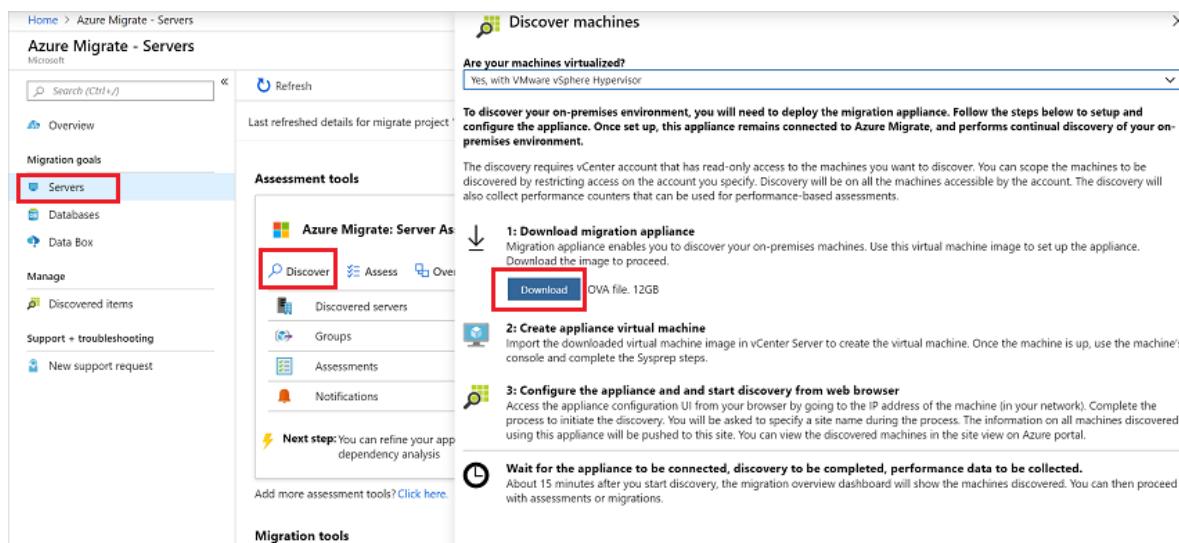
Skip adding an assessment tool for now

9. In **Select migration tool**, select **Skip adding a migration tool for now > Next**.
10. In **Review + add tools**, review the settings, then select **Add tools**.

- Wait a few minutes for the Azure Migrate project to deploy. You'll be taken to the project page. If you don't see the project, you can access it from **Servers** in the Azure Migrate dashboard.

## Download the collector appliance

- In **Migration Goals > Servers > Azure Migrate: Server Assessment**, select **Discover**.
- In **Discover machines > Are your machines virtualized?**, select **Yes, with VMware vSphere hypervisor**.
- Select **Download** to download the .OVA template file.



## Verify the collector appliance

Before deploying the VM, Contoso checks that the OVA file is secure:

- On the machine on which the file was downloaded, Contoso opens an administrator Command Prompt window.
- Contoso runs the following command to generate the hash for the OVA file:

```
C:\> CertUtil -HashFile <file_location> [Hashing Algorithm]
```

**Example:**

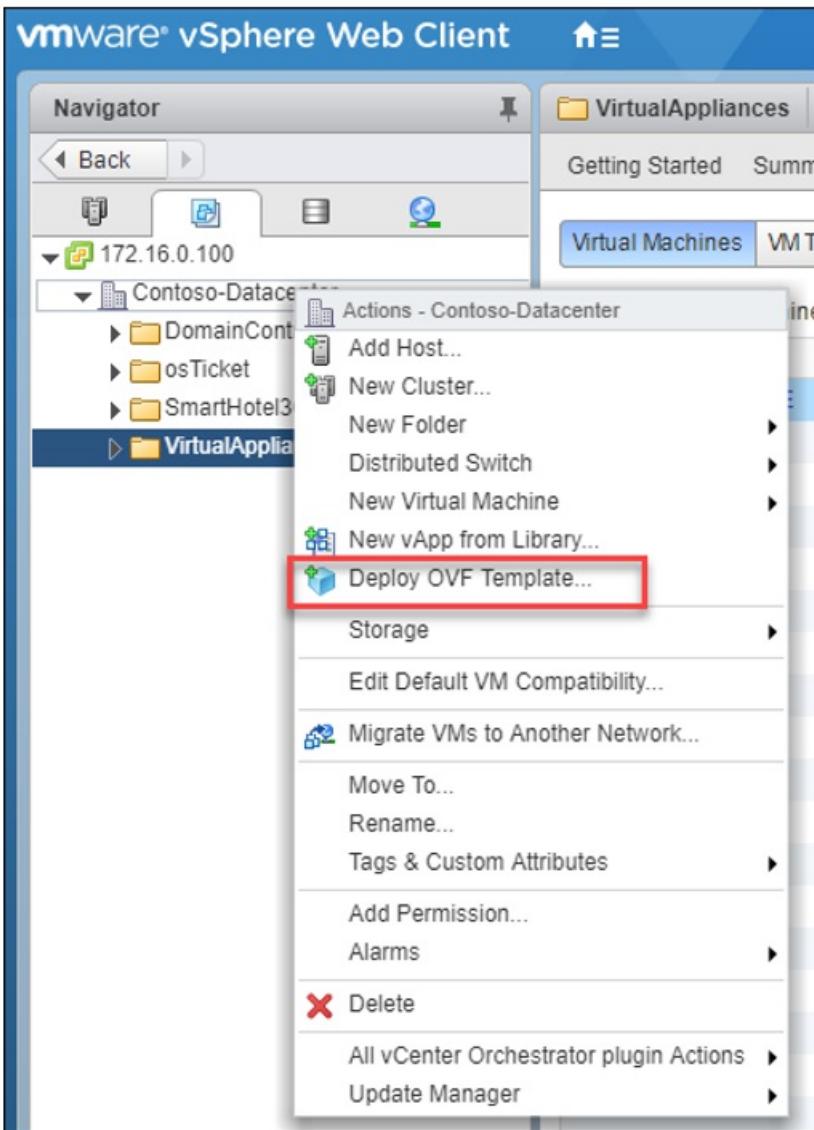
```
C:\> CertUtil -HashFile C:\AzureMigrate\AzureMigrate.ova SHA256
```

- The generated hash should match the hash values listed in the [Verify security](#) section of the [Assess VMware VMs for migration](#) tutorial.

## Create the collector appliance

Now, Contoso can import the downloaded file to the vCenter Server instance and provision the collector appliance VM:

- In the vSphere Client console, Contoso selects **File > Deploy OVF template**.

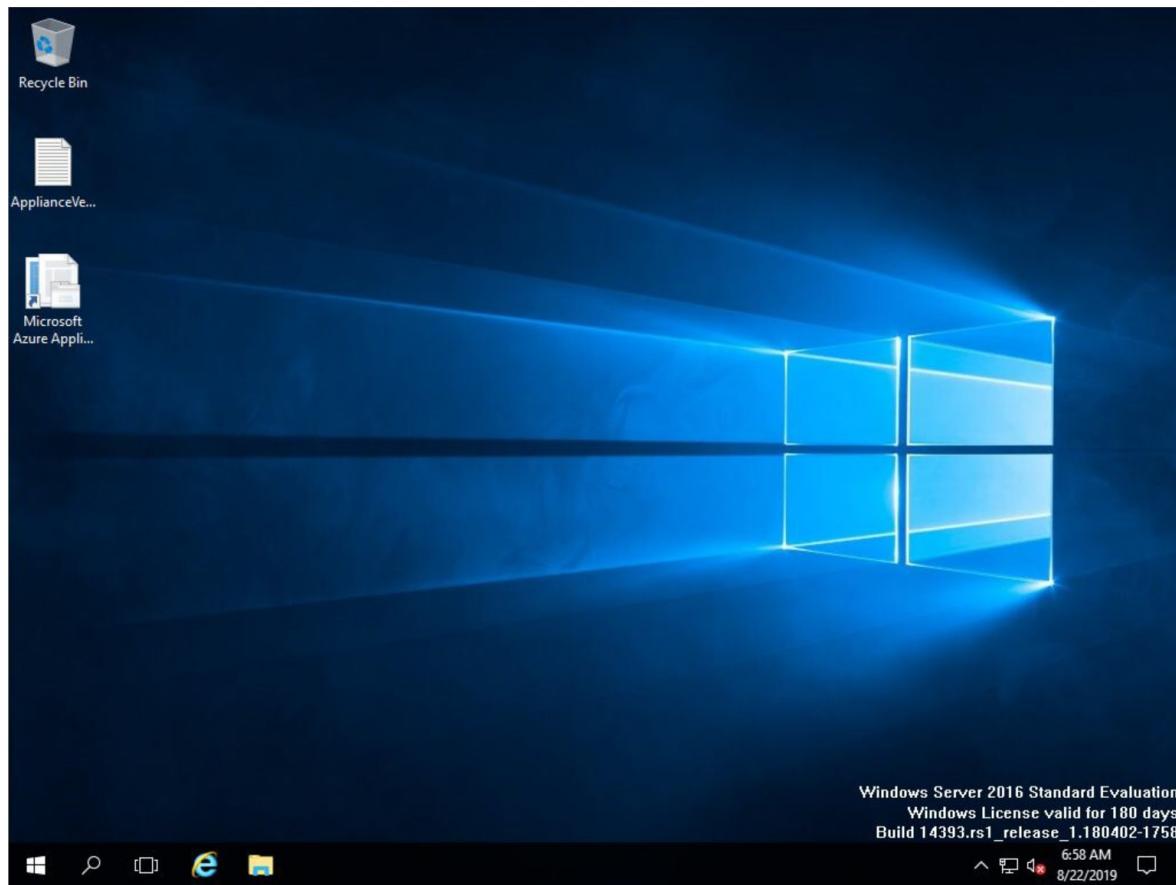


2. In the Deploy OVF Template Wizard, Contoso selects **Source**, and then specifies the location of the OVA file.
3. In **Name and Location**, Contoso specifies a display name for the collector VM. Then, it selects the inventory location in which to host the VM. Contoso also specifies the host or cluster on which to run the collector appliance.
4. In **Storage**, Contoso specifies the storage location. In **Disk Format**, Contoso selects how it wants to provision the storage.
5. In **Network Mapping**, Contoso specifies the network in which to connect the collector VM. The network needs internet connectivity to send metadata to Azure.
6. Contoso reviews the settings, then selects **Power on after deployment > Finish**. A message that confirms successful completion appears when the appliance is created.

#### Run the collector to discover VMs

Now, Contoso runs the collector to discover VMs. Currently, the collector currently supports only **English (United States)** as the operating system language and collector interface language.

1. In the vSphere Client console, Contoso selects **Open Console**. Contoso specifies the accepts the licensing terms, and password preferences for the collector VM.
2. On the desktop, Contoso selects the **Microsoft Azure Appliance Configuration Manager** shortcut.



3. In the Azure Migrate Collector, Contoso selects **Set up prerequisites**. Contoso accepts the license terms and reads the third-party information.
4. The collector checks that the VM has internet access, that the time is synced, and that the collector service is running. (The collector service is installed by default on the VM.) Contoso also installs the VMware vSphere Virtual Disk Development Kit.

**NOTE**

It's assumed that the VM has direct access to the internet without using a proxy.



### Set up prerequisites

Verify and set up appliance prerequisites



Accepted license terms



You are connected to the Internet



Time in sync with the Internet time server



Latest Azure Migrate updates are installed



VMware vSphere Virtual Disk Development Kit is installed

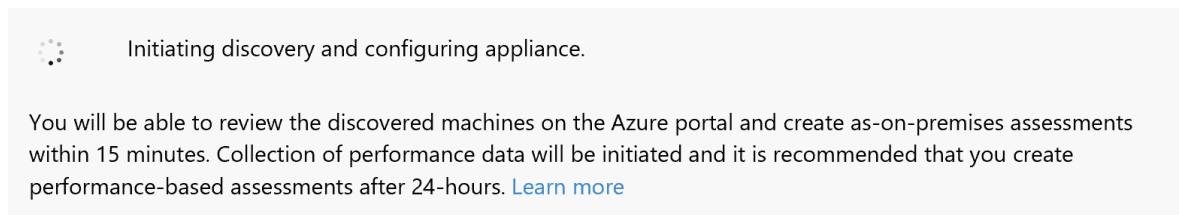
5. Sign into your Azure account and select the subscription and Migrate project you created earlier. Also enter a name for the **appliance** so you can identify it in the Azure portal.
6. In **Specify vCenter Server details**, Contoso enters the name (FQDN) or IP address of the vCenter

Server instance and the read-only credentials used for discovery.

7. Contoso selects a scope for VM discovery. The collector can discover only VMs that are within the specified scope. The scope can be set to a specific folder, datacenter, or cluster.

The screenshot shows the 'Specify vCenter Server details' dialog. At the top, there's a green checkmark icon and the title 'Specify vCenter Server details'. Below it is a sub-instruction: 'Connect to vCenter Server and select a scope for collection'. The main section is titled 'Connect to vCenter Server' with the sub-instruction 'Specify a read-only account for accessing vCenter Server'. It contains fields for 'vCenter Server name or IP address' (192.168.0.101), 'Username' (administrator@contoso.com), and 'Password' (redacted). A 'Connect' button is highlighted in blue, and next to it is a green checkmark icon with the word 'Connected'. Below this section is another titled 'Select scope' with the sub-instruction 'Selecting a scope enables collection for a subset of virtual machines'. It shows a dropdown menu under 'Hosts and Clusters' containing 'Contoso-Datacenter' and a note below it stating 'Contoso-Datacenter has 6 virtual machines'.

8. The collector will now start to discovery and collect information about the Contoso environment.



### Verify VMs in the portal

When collection is finished, Contoso checks that the VMs appear in the portal:

1. In the Azure Migrate project, Contoso selects **Servers** servers\*\*. Contoso checks that the VMs that it wants to discover are shown.

✓ Discovery is complete for session ID: 576abe81-1a3d-4726-9e3f-950b79dcdecf at 5/27/2018, 3:33:42 PM. Use 'Create assessment' command to create an assessment.

Search to filter machines

NAME	DEPENDENCIES	CORES	MEMORY (MB)	DISKS	STORAGE (GB)	NETWORK ADAPTERS	OPERATING SYSTEM
OSTICKETMYSQL	<a href="#">i Requires agent installation</a>	2	4096	1	16	1	Ubuntu Linux (64-bit)
OSTICKETWEB	<a href="#">i Requires agent installation</a>	2	4096	1	16	1	Ubuntu Linux (64-bit)
CONTOSODC1	<a href="#">i Requires agent installation</a>	4	4096	1	40	1	Microsoft Windows Server 2016 (64-bit)
vcenter	<a href="#">i Requires agent installation</a>	2	10240	12	229	1	Other 3.x or later Linux (64-bit)
CONTOSOGW	<a href="#">i Requires agent installation</a>	4	4096	1	40	2	Microsoft Windows Server 2016 (64-bit)
CONTOSODC2	<a href="#">i Requires agent installation</a>	4	4096	1	40	1	Microsoft Windows Server 2016 (64-bit)
WEBVM	<a href="#">i Requires agent installation</a>	4	4096	1	40	1	Microsoft Windows Server 2008 R2 (64-bit)
AZUREMIGRATE	<a href="#">i Requires agent installation</a>	4	8192	1	80	1	Microsoft Windows Server 2012 (64-bit)
SQLVM	<a href="#">i Requires agent installation</a>	4	4096	1	40	1	Microsoft Windows Server 2008 R2 (64-bit)

2. Currently, the machines don't have the Azure Migrate agents installed. Contoso must install the agents to view dependencies.

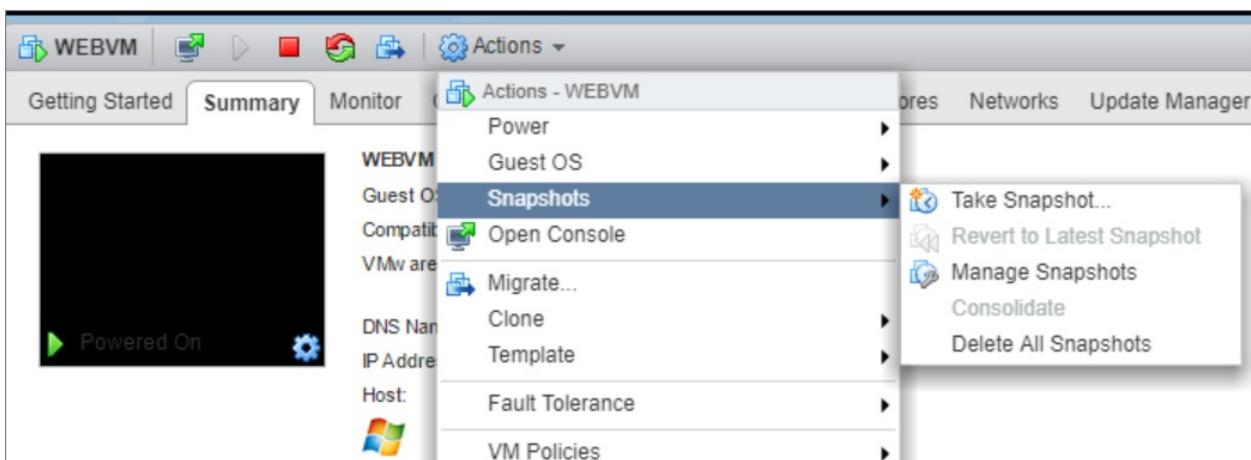
NAME	DEPENDENCIES
OSTICKETMYSQL	<a href="#">i Requires agent installation</a>
OSTICKETWEB	<a href="#">i Requires agent installation</a>
CONTOSODC1	<a href="#">i Requires agent installation</a>
vcenter	<a href="#">i Requires agent installation</a>
CONTOSOGW	<a href="#">i Requires agent installation</a>
CONTOSODC2	<a href="#">i Requires agent installation</a>
WEBVM	<a href="#">i Requires agent installation</a>
AZUREMIGRATE	<a href="#">i Requires agent installation</a>
SQLVM	<a href="#">i Requires agent installation</a>

## Step 5: Prepare for dependency analysis

To view dependencies between VMs that it wants to assess, Contoso downloads and installs agents on the app VMs. Contoso installs agents on all VMs for its apps, both for Windows and Linux.

### Take a snapshot

To keep a copy of the VMs before modifying them, Contoso takes a snapshot before the agents are installed.



## Download and install the VM agents

1. In Machines, Contoso selects the machine. In the Dependencies column, Contoso selects **Requires installation**.
2. In the **Discover machines** pane, Contoso:
  - Downloads the Microsoft Monitoring Agent and the Microsoft Dependency Agent for each Windows VM.
  - Downloads the Microsoft Monitoring Agent and Microsoft Dependency Agent for each Linux VM.
3. Contoso copies the workspace ID and key. Contoso needs the workspace ID and key when it installs the Microsoft Monitoring Agent.

Dependency visualization of machines requires a deeper discovery which involves installation and configuration

Once the installation of the agents is done, it may take up to 15 minutes to reflect in the Azure Migrate portal.

### Step 1: Download & install Microsoft Monitoring Agent (MMA)

1. [Windows 64-bit](#)
2. [Linux](#)

[Learn more](#) about installation of MMA agent.

### Step 2: Download and install dependency agent

1. [Windows 64-bit](#)
2. [Linux](#)

[Learn more](#) about installation of dependency agent.

If you have machines with no internet connectivity to OMS, you need to download and install OMS gateway.

[Learn more](#)

### Step 3: Configure MMA agent

Configure MMA agent with the workspace by specifying the below workspace ID and key.

[Learn more](#)

Workspace ID:

Workspace key:

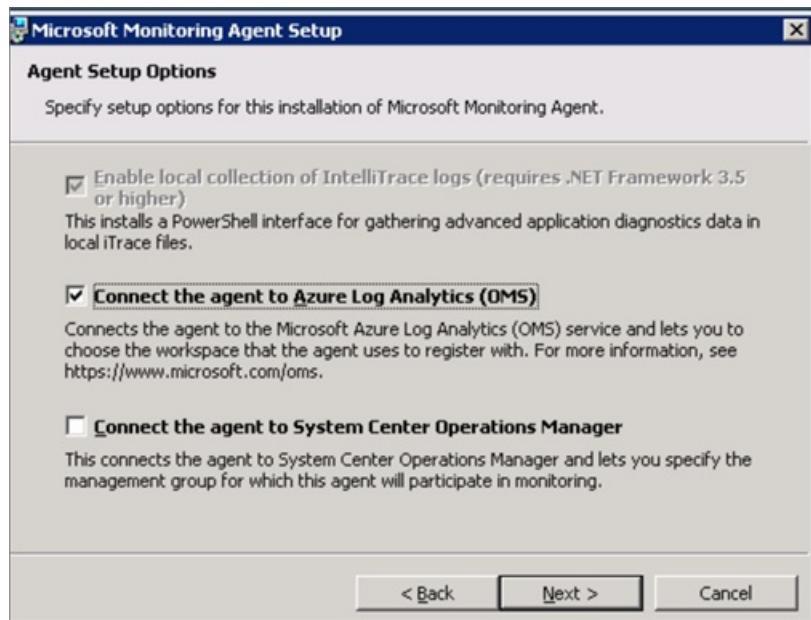
 

## Install the agents on Windows VMs

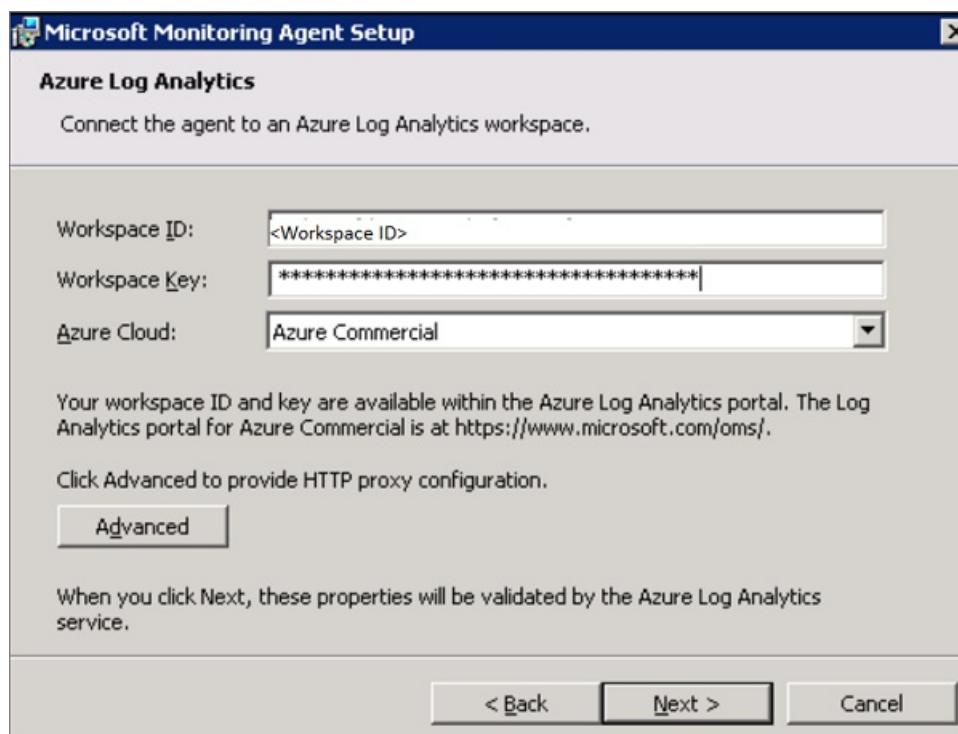
Contoso runs the installation on each VM.

### Install the MMA on Windows VMs

1. Contoso double-clicks the downloaded agent.
2. In **Destination Folder**, Contoso keeps the default installation folder, and selects **Next**.
3. In **Agent Setup Options**, Contoso selects **Connect the agent to Azure Log Analytics** > **Next**.



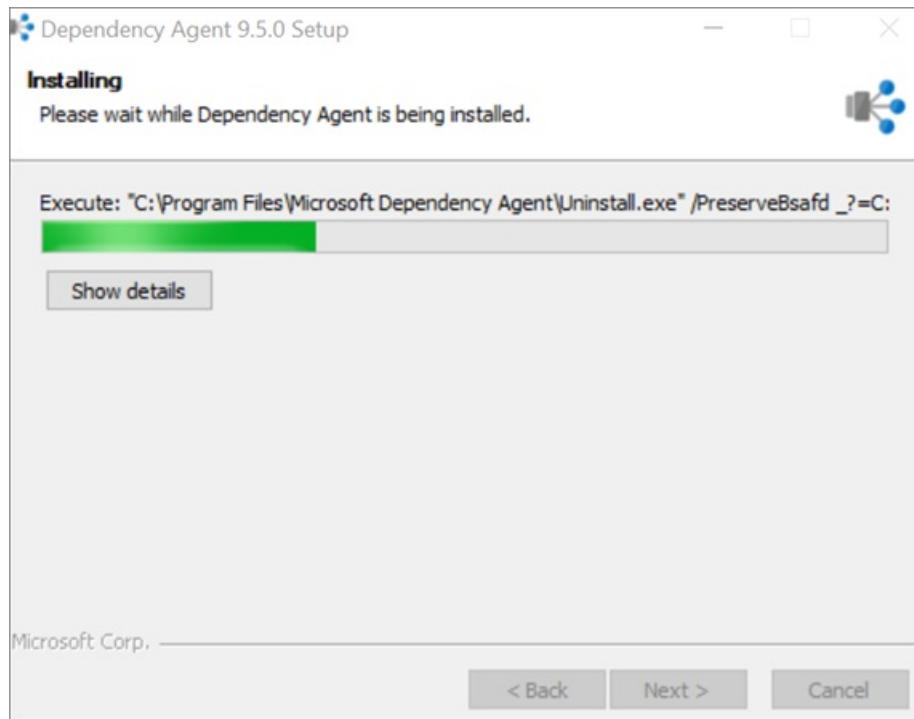
4. In Azure Log Analytics, Contoso pastes the workspace ID and key that it copied from the portal.



5. In Ready to Install, Contoso installs the MMA.

#### Install the Microsoft Dependency Agent on Windows VMs

1. Contoso double-clicks the downloaded agent.
2. Contoso accepts the license terms and waits for the installation to finish.



## Install the agents on Linux VMs

Contoso runs the installation on each VM.

### Install the MMA on Linux VMs

1. Contoso installs the Python ctypes library on each VM by using the following command:

```
sudo apt-get install python-ctypeslib
```

2. Contoso must run the command to install the MMA agent as root. To become root, Contoso runs the following command, and then enters the root password:

```
sudo -i
```

3. Contoso installs the MMA:

- Contoso enters the workspace ID and key in the command.
- Commands are for 64-bit.
- The workspace ID and primary key are located in the Log Analytics workspace in the Azure portal. Select **Settings**, and select the **Connected Sources** tab.
- Run the following commands to download the Log Analytics agent, validate the checksum, and install and onboard the agent:

```
wget https://raw.githubusercontent.com/Microsoft/OMS-Agent-for-Linux/master/installer/scripts/onboard_agent.sh && sh onboard_agent.sh -w 6b7fcaff-7efb-4356-ae06-516cacf5e25d -s  
k7gAMAw5Bk8pFVUTZKmk2lG4eUciswzWfYLDTxGcD8pcyc4oT8c6ZRgsMy3MmsQSHuSOcmBUsCjoRiG2x9A8Mg==
```

### Install the Microsoft Dependency Agent on Linux VMs

After the Microsoft Monitoring Agent is installed, Contoso installs the Microsoft Dependency Agent on the Linux VMs:

1. The Microsoft Dependency Agent is installed on Linux computers by using

`InstallDependencyAgent-Linux64.bin`, a shell script that has a self-extracting binary. Contoso runs the file by using `sh`, or it adds execute permissions to the file itself.

2. Contoso installs the Linux dependency agent as root:

```
wget --content-disposition https://aka.ms/dependencyagentlinux -O InstallDependencyAgent-Linux64.bin &&
sudo sh InstallDependencyAgent-Linux64.bin -s
```

## Step 6: Run and analyze the VM assessment

Contoso can now verify machine dependencies and create a group. Then, it runs the assessment for the group.

### Verify dependencies and create a group

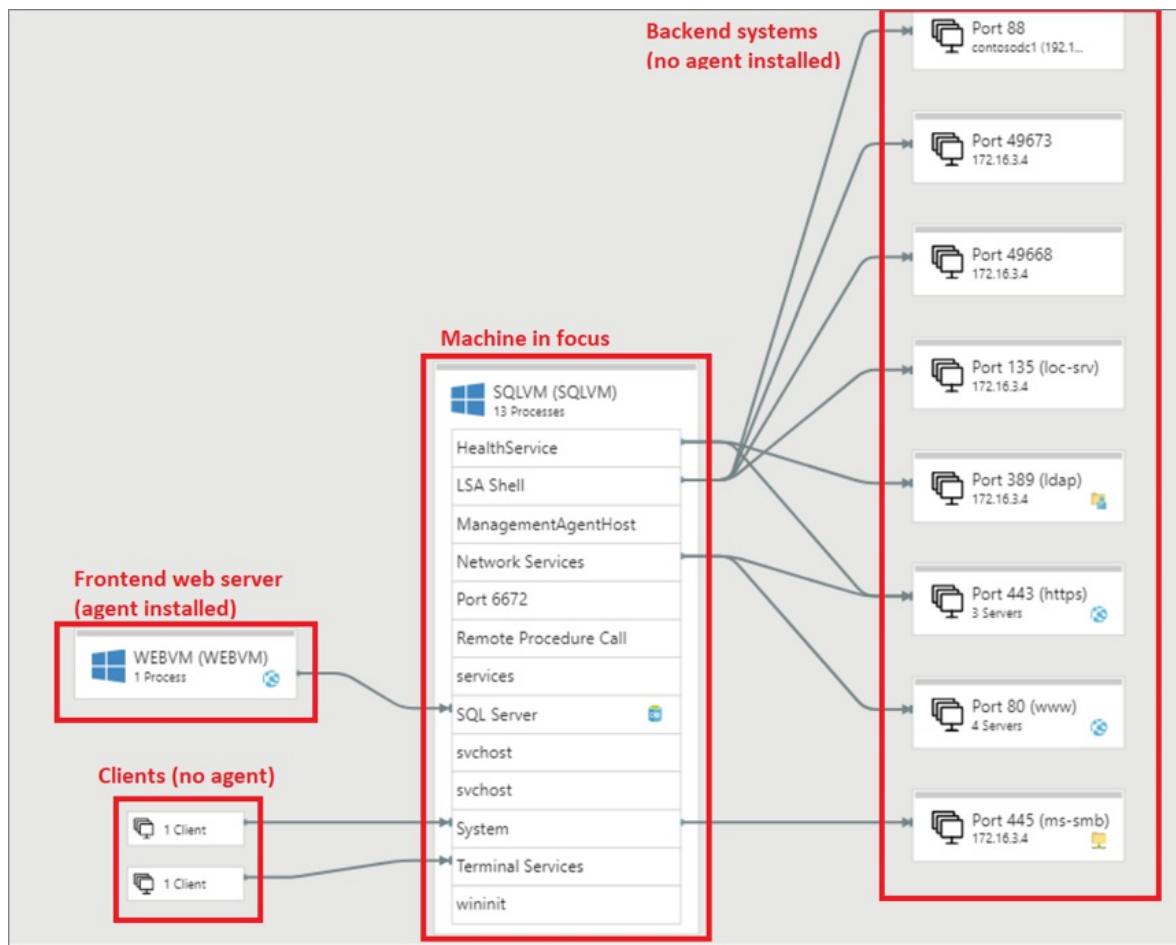
1. To determine which machines to analyze, Contoso selects **View Dependencies**.

NAME	MEMBER OF	DEPENDENCIES
AzureMigrate		Requires agent installation
SQLVM		View dependencies
contosogw		Requires agent installation
vcenter		Requires agent installation
WEBVM		View dependencies
contosodc1		Requires agent installation

2. For SQLVM, the dependency map shows the following details:

- Process groups or processes that have active network connections running on SQLVM during the specified time period (an hour, by default).
- Inbound (client) and outbound (server) TCP connections to and from all dependent machines.
- Dependent machines that have the Azure Migrate agents installed are shown as separate boxes.
- Machines that don't have the agents installed show port and IP address information.

3. For machines that have the agent installed (`WEBVM`), Contoso selects the machine box to view more information. The information includes the FQDN, operating system, and MAC address.



- Contoso selects the VMs to add to the group (`SQLVM` and `WEBVM`). Contoso holds the `Ctrl` key while selecting multiple VMs.
- Contoso selects **Create Group**, and then enters a name (`smarthotelapp`).

#### NOTE

To view more granular dependencies, you can expand the time range. You can select a specific duration or select start and end dates.

#### Run an assessment

- In **Groups**, Contoso opens the group (`smarthotelapp`), then selects **Create assessment**.

The screenshot shows the Azure Migrate interface. At the top, there's a navigation bar with 'Home', 'Migration projects', 'ContosoPOC', 'Groups', and 'smarthotelapp'. Below the navigation is a toolbar with 'Add machines', 'Remove machines', 'Refresh', 'Create assessment' (which is highlighted with a red box), 'View assessments', 'View dependencies', 'Columns', and 'Delete group'. A status bar indicates 'Group status: Created (Friday, April 13, 2018, 3:50:14 AM)'. Under the toolbar, there's a summary: 'Machines: 2' (with icons for Windows and Linux) and 'Assessments: 1'. The main area is titled 'MACHINES' and contains a table:

NAME	MEMBER OF	DEPENDENCY AGENT	CORES	MEMORY (MB)	DISKS	STORAGE (GB)	NETWORK ADAPTERS	OPERATING SYSTEM
SQLVM	smarthotelapp	✓ Installed	4	4096	1	40	1	Microsoft Windows Server 200...
WEBVM	smarthotelapp	✓ Installed	4	4096	1	40	1	Microsoft Windows Server 200...

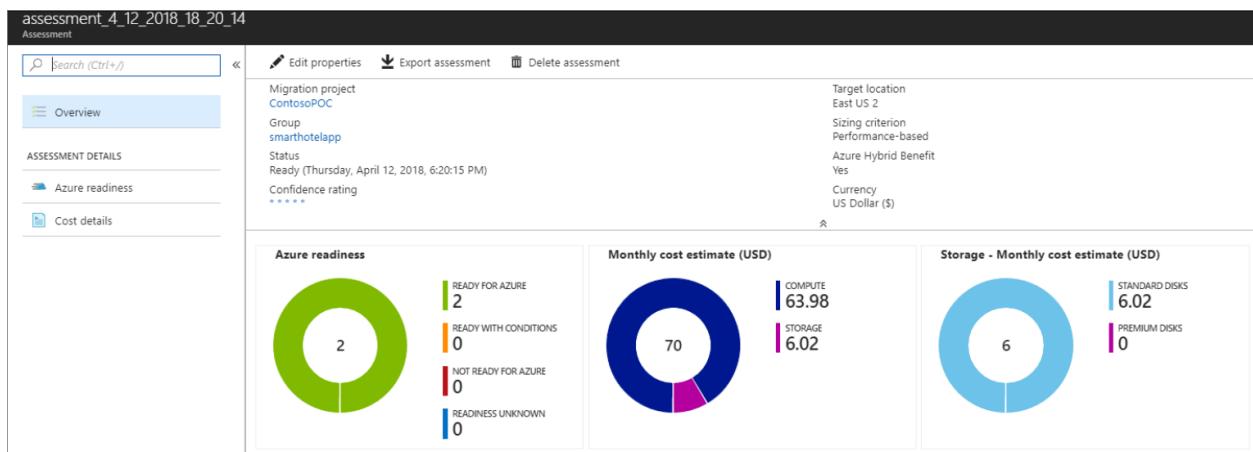
- To view the assessment, Contoso selects **Manage > Assessments**.

Contoso uses the default assessment settings, but you can [customize settings](#).

#### Analyze the VM assessment

An Azure Migrate assessment includes information about the compatibility of on-premises with Azure, suggested

right-sizing for Azure VM, and estimated monthly Azure costs.



#### Review confidence rating

Machines	Assessments	Groups								
6	1	1								
Assessments										
<table border="1"> <thead> <tr> <th>NAME</th><th>GROUP</th><th>STATUS</th><th>CONFIDENCE RATING</th></tr> </thead> <tbody> <tr> <td>assessment_4_12_2018_18_20_14</td><td>smarthotelapp</td><td> Ready (4/12/2018, 6:20:15 PM)</td><td></td></tr> </tbody> </table>			NAME	GROUP	STATUS	CONFIDENCE RATING	assessment_4_12_2018_18_20_14	smarthotelapp	Ready (4/12/2018, 6:20:15 PM)	
NAME	GROUP	STATUS	CONFIDENCE RATING							
assessment_4_12_2018_18_20_14	smarthotelapp	Ready (4/12/2018, 6:20:15 PM)								
Groups										
<table border="1"> <thead> <tr> <th>NAME</th><th>TOTAL MACHINES</th><th>LAST UPDATED DATE</th></tr> </thead> <tbody> <tr> <td>smarthotelapp</td><td>2</td><td>4/12/2018, 6:20:20 PM</td></tr> </tbody> </table>			NAME	TOTAL MACHINES	LAST UPDATED DATE	smarthotelapp	2	4/12/2018, 6:20:20 PM		
NAME	TOTAL MACHINES	LAST UPDATED DATE								
smarthotelapp	2	4/12/2018, 6:20:20 PM								

An assessment has a confidence rating of from 1 star to 5 stars (1 star is the lowest and 5 stars is the highest).

- The confidence rating is assigned to an assessment based on the availability of data points that are needed to compute the assessment.
- The rating helps you estimate the reliability of the size recommendations that are provided by Azure Migrate.
- The confidence rating is useful when you are doing *performance-based sizing*. Azure Migrate might not have enough data points for utilization-based sizing. For *as on-premises* sizing, the confidence rating is always 5 stars because Azure Migrate has all the data points it needs to size the VM.
- Depending on the percentage of data points available, the confidence rating for the assessment is provided:

AVAILABILITY OF DATA POINTS	CONFIDENCE RATING
0%-20%	1 star
21%-40%	2 stars

AVAILABILITY OF DATA POINTS	CONFIDENCE RATING
41%-60%	3 stars
61%-80%	4 stars
81%-100%	5 stars

## Verify Azure readiness

Azure readiness

Category	Count
READY FOR AZURE	2
READY WITH CONDITIONS	0
NOT READY FOR AZURE	0
READINESS UNKNOWN	0

Details [How do I modify list of assessed machines?](#)

i Finished retrieving data.

Search to filter machines

NAME	AZURE VM READINESS	AZURE VM SIZE	SUGGESTED TOOL	OPERATING SYSTEM	BOOT TYPE	DISKS ON-PREMISES	STORAGE ON-PREMISES (G...)
SQLVM	✓	Standard_A1_v2	<a href="#">Azure Database Mig...</a>	Microsoft Windows Ser...	BIOS	1	40
WEBVM	✓	Standard_A1_v2	<a href="#">Azure Site Recovery</a>	Microsoft Windows Ser...	BIOS	1	40

The assessment report shows the information that's summarized in the table. To show performance-based sizing, Azure Migrate needs the following information. If the information can't be collected, sizing assessment might not be accurate.

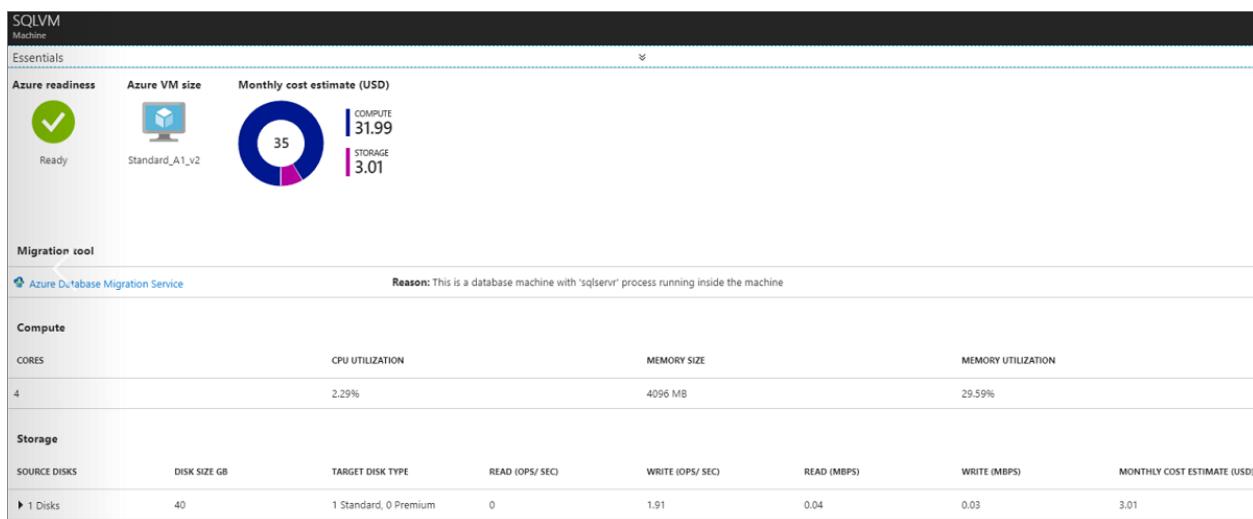
- Utilization data for CPU and memory.
- Read/write IOPS and throughput for each disk attached to the VM.
- Network in/out information for each network adapter attached to the VM.

SETTING	INDICATION	DETAILS
Azure VM readiness	Indicates whether the VM is ready for migration.	<p>Possible states:</p> <ul style="list-style-type: none"> <li>Ready for Azure</li> <li>Ready with conditions</li> <li>Not ready for Azure</li> <li>Readiness unknown</li> </ul> <p>If a VM isn't ready, Azure Migrate shows some remediation steps.</p>
Azure VM size	For ready VMs, Azure Migrate provides an Azure VM size recommendation.	<p>Sizing recommendation depends on assessment properties:</p> <ul style="list-style-type: none"> <li>If you used performance-based sizing, then sizing considers the performance history of the VMs.</li> <li>If you used <i>as on-premises</i> sizing, then sizing is based on the on-premises VM size and utilization.</li> <li>Data isn't used.</li> </ul>

SETTING	INDICATION	DETAILS
Suggested tool	Because Azure machines are running the agents, Azure Migrate looks at the processes that are running inside the machine. It identifies whether the machine is a database machine.	
VM information	The report shows settings for the on-premises VM, including operating system, boot type, and disk and storage information.	

#### Review monthly cost estimates

This view shows the total compute and storage cost of running the VMs in Azure. It also shows details for each machine.



- Cost estimates are calculated by using the size recommendations for a machine.
- Estimated monthly costs for compute and storage are aggregated for all VMs in the group.

## Clean up after assessment

- When the assessment finishes, Contoso retains the Azure Migrate appliance to use in future evaluations.
- Contoso turns off the VMware VM. Contoso will use it again when it evaluates additional VMs.
- Contoso keeps the `Contoso Migration` project in Azure. The project currently is deployed in the `ContosoFailoverRG` resource group in the East US Azure region.
- The collector VM has a 180-day evaluation license. If this limit expires, Contoso will need to download the collector and set it up again.

## Conclusion

In this scenario, Contoso assesses its SmartHotel360 app database by using the Data Migration Assistant tool. It assesses the on-premises VMs by using the Azure Migrate service. Contoso reviews the assessments to make sure that on-premises resources are ready for migration to Azure.

## Next steps

After Contoso assesses this workload as a potential migration candidate, it can begin preparing its on-premises infrastructure and its Azure infrastructure for migration. See the [deploy Azure infrastructure](#) article in the Cloud Adoption Framework migrate best practices section for an example of how Contoso performs these processes.



# Plan a data warehouse migration

11/9/2020 • 14 minutes to read • [Edit Online](#)

A data warehouse migration is a challenge for any company. In order to execute it well and avoid any unwelcome surprises and unplanned costs, you need to thoroughly research the challenge, mitigate risk, and plan your migration to ensure that you're as ready as possible. At a high level, your plan should cover the core data warehouse migration process steps and any tasks within them. The main process steps are:

- Pre-migration preparation
- Migration strategy and execution
- Post-migration

For example, preparation includes things like readying your data warehouse migration team in terms of skills training and technology familiarization. It also includes setting up a proof of concept lab, understanding how you will manage test and production environments, gaining appropriate clearance to migrate your data and a production system outside of the corporate firewall and setting up migration software in your datacenter to enable migration to proceed.

For a data warehouse migration to proceed smoothly, your plan should establish a clear understanding of:

- Your business case, including its drivers, business benefits, and risks.
- Migration team roles and responsibilities.
- The skill set and training required to enable successful migration.
- Allocated budget for the complete migration.
- Your migration strategy.
- How you can avoid risk in the migration project to avoid delays or rework.
- Your existing data warehouse system, its architecture, schema, data volumes, data flows, security, and operational dependencies.
- Differences between your existing on premises data warehouse DBMS and Azure Synapse, like data types, SQL functions, logic, and other considerations.
- What needs to be migrated and priorities.
- The migration tasks, approaches, order, and deadlines.
- How you will control migration.
- How to prevent user disruption while undertaking the migration.
- What you need to do on-premises to avoid delays and enable migration.
- Tools to enable secure migration of schemas, data, and ETL processing to Azure.
- Data model design changes that are required during and after migration.
- Any pre-migration or post-migration technology changes and how to minimize rework.
- Post-migration technology deprecation.
- How you will implement testing and quality assurance to prove success.
- Your checkpoints to assess progress and enable decisions to be made.
- Your contingency plan and points of rollback in case things go wrong.

In order to achieve this understanding, we need to prepare and begin specific activities before any migration starts. Let's look at what that entails in more detail.

## Pre-migration preparation

There are several things that should be addressed before you even begin a data warehouse migration.

## **Key roles in a data warehouse migration team**

Key roles in a migration project include:

- Business owner
- Project manager (with agile methodology experience such as Scrum)
- Project coordinator
- Cloud engineer
- Database administrator (existing data warehouse DBMS and Azure Synapse)
- Data modelers
- ETL developers
- Data virtualization specialist (could be a DBA)
- Testing engineer
- Business analysts (to help test BI tool queries, reports, and analyses)

In addition, the team need the support of your on-premises infrastructure team.

## **Skills and training to ready the team for migration**

With respect to skills, expertise is important in a data warehouse migration. Therefore, ensure the appropriate members of your migration team are trained in Azure cloud fundamentals, Azure Blob storage, Azure Data Lake Storage, Azure Data Box, ExpressRoute, Azure identity management, Azure Data Factory, and Azure Synapse. Your data modelers will most likely need to fine-tune your Microsoft Azure Synapse data models once migration from your existing data warehouse has occurred.

## **Assessing your existing data warehouse**

Another part of preparing to migrate is the need for a full assessment of your existing data warehouse to fully understand the architecture, data stores, schema, business logic, data flows, the DBMS functionality utilized, warehouse operation, and the dependencies. The more understanding is gained here the better. A detailed knowledge of how the system works helps to communicate and cover off all bases.

The purpose of the assessment is not just to ensure detailed understanding of the current setup across the migration team but also to understand strengths and weaknesses in the current setup. The outcome of an assessment of your current data warehouse therefore can impact your migration strategy in terms of lift and shift versus something broader. For example, if the outcome of an assessment is that your data warehouse is at end of life then clearly the strategy would be more of a data migration to a newly designed data warehouse on Azure Synapse versus a lift and shift approach.

## **On-premises preparation for data migration**

In addition to preparing and readying your migration team for your target environment and assessing your current setup, it is equally important to also set things in motion on-premises as production data warehouses tend to be heavily controlled by IT procedures and approval processes. To avoid delays, ensure that your datacenter infrastructure and operations teams are ready for migrating your data, schema, ETL jobs, and so on, to the Azure cloud. Data migration can occur via:

- AzCopy to Azure Blob storage.
- Microsoft Azure ExpressRoute to transfer compressed data directly to Azure.
- File export to Azure Data Box.

The main factors influencing which of these options is selected are data volume size (in terabytes) and network speed (in Mbps). A calculation is needed to determine how long it would take to migrate the data via the network, considering that data might be compressed in your data warehouse and become uncompressed when you export it. This situation can slow data transfer. Recompress data via Gzip when moving data by any of the above methods. PolyBase can process gzipped data directly. Large data volumes will likely be migrated via Azure Data Box if it will

take too long to move the data.

Additionally, for Azure Data Factory to control the execution of exports of your existing data warehouse data from Azure, self-hosted integration run-time software must be installed in your datacenter to enable migration to proceed. Given these requirements if formal approval is needed to make this possible, then starting the appropriate approval processes early to enable this to happen will help avoid delays down the line.

### Azure preparation for schema and data migration

In terms of preparation on the Azure side, data import will need to be managed either via Microsoft Azure ExpressRoute or Microsoft Azure Data Box. Azure Data Factory pipelines are an ideal way to load your data into Azure Blob Storage and then load from there into Azure Synapse using PolyBase. Therefore preparation is needed on the Azure side to develop such a pipeline.

The alternative is to use your existing ETL tool on Azure if it supports Azure Synapse, which means setting up the tool on Azure from Azure Marketplace and readying a pipeline to import your data and load it into Azure Blob storage.

## Defining a migration strategy

### Migration goals

In any strategy, there needs to be a set of objectives or goals that should be defined to indicate success. Targets can then be set to achieve these goals and people given responsibility for reaching them. Examples of migration goals and corresponding metrics to set targets for in a cloud data warehouse migration project are shown in the table below:

Types of goal and metric examples:

#### Improve overall performance

- Data migration performance
- ELT performance
- Data loading performance
- Complex query performance
- Number of concurrent users

#### Run at lower cost

- Cost of compute by workload, for example, number of compute hours x cost per hour for:
  - Standard reporting
  - Ad hoc queries
  - Batch ELT processing
- Cost of storage (staging, production tables, indexes, temporary space)

#### Operate with better availability and service levels

- Service level agreements
- High availability

#### Improve productively

- Tasks automated, reduced administrative headcount

A successful data warehouse migration can therefore be interpreted as a data warehouse that runs as fast or faster and at lower cost than the legacy system you migrated from. Assigning owners of these goals creates accountability for reaching them. It also ensures that testing in a proof of concept lab (as defined in the de-risking section in this guide) will be deemed successful if the tests identify ways that the goals can be achieved.

### Migration approach

You have several strategic options for migrating your existing data warehouse to Azure Synapse:

- Lift and shift your existing data warehouse as-is.
- Simplify your existing data warehouse and then migrate it.
- Completely redesign your data warehouse on Azure Synapse and migrate your data.

The findings of the assessment of your existing data warehouse should significantly influence your strategy. A good assessment outcome might recommend a lift and shift strategy. A mediocre outcome due to a low agility rating might indicate that simplification is needed before migration. A poor outcome might indicate a complete redesign is needed.

Lift and shift leaves your architecture as-is, trying to minimize the work in moving your existing system. If your existing ETL tool already supports Azure Synapse, you might be able to change the target with minimal effort. Nevertheless there will be differences in table types, data types, SQL functions, views, stored procedure business logic etc. These differences and ways around them are detailed in lower-level documents in this migration series.

Simplifying your existing data warehouse prior to migration is about reducing complexity to ease migration. It could include:

- Removing or archiving unused tables before migrating to avoid migrating data that is not used.
- Converting physical data marts to virtual data marts using data virtualization software to reduce what you have to migrate. Conversion also improves agility and reduces total cost of ownership, so it could be considered as modernization during migration.

You can also simplify first and then lift and shift what remains.

## **Migration scope**

Whatever strategy you choose, you should clearly define the scope of the migration, what will be migrated, and whether you'll migrate incrementally or all at once. One example of incremental migration is migrating your data marts first, followed by your data warehouse. This approach would allow you to focus on high-priority business areas while allowing your team to incrementally build expertise as each mart is individually migrated, before migrating the data warehouse itself.

## **Defining what has to be migrated**

Make an inventory of everything that needs to be migrated. This includes schema, data, ETL processes (pipelines), authorization privileges, users, BI tool semantic access layers, and analytic applications. A detail understanding of what's involved in migrating the inventory is provided in each of the lower-level migration articles in this series. Links to these are shown below.

- Schema migration, design, and performance considerations.
- Data migration, ETL processing, and load.
- Access security and data warehouse operations.
- Migration of visualization and reports.
- Minimizing the impact of SQL issues.
- Third-party tools to help you in your data warehouse migration.

If you are uncertain about the best approach, conduct tests in a proof of concept lab to identify optimal techniques. For more information, see the section on de-risking your data warehouse migration project.

## **Migration control**

Data warehouse migration to Azure Synapse involves tasks that need to be conducted:

- On-premises, such as data export.
- On the network, such as data transfer.
- In the Azure cloud, such as data transformation, integration, and load.

The problem is that managing these tasks can be complicated if scripts and utilities are all being developed, tested,

and run independently in both on-premises and Azure environments. It adds complexity especially if version control, test management and migration execution are not coordinated.

You should avoid these complexities and control them from a common place via a source control repository to manage change from development to testing and production. Migration execution will involve tasks that need to be performed on-premises, on the network, and in Azure. Because Azure Synapse is the target environment, controlling migration execution from Azure simplifies management. Use Azure Data Factory (ADF) to create a migration control pipeline to control execution both on-premises and on Azure. This introduces automation and minimizes errors. ADF becomes a migration orchestration tool, not just an enterprise data integration tool.

Other options to control migration available from Microsoft partners running on Azure include data warehouse automation tools to try to automate migration. Vendors like WhereScape and Attunity for example. Most of these automation tools are aimed at a lift and shift approach to migration. Even then, there may be some things that may not be supported by such tools, for example, stored procedures. These products and several others are detailed in a separate guide dedicated to third-party tools to help you migrate to Azure Synapse.

## Migration testing

The first thing you need for testing is to define a series of tests and a set of required outcomes for each test that need to be run to verify and indicate success. It is important to ensure that all aspects are tested and compared across your existing and migrated systems including:

- Schema
- Data types converted where necessary
- Use user-defined schema in Azure Synapse to distinguish between data warehouse and data mart tables
- Users
- Roles and assignments of users to those roles
- Data access security privileges
- Data privacy and compliance
- Privileges that govern administration capabilities
- Data quality and integrity
- ETL processing that populates Azure Synapse both into the data warehouse and from the data warehouse to any data marts, including testing
- All rows are correct in all tables including history
- Slowly changing dimension processing
- Change data capture processing
- Calculations and aggregations that use functions that could differ across systems
- Results of all known queries, reports, and dashboards
- Performance and scalability
- Analytical functionality
- Costs in the new pay-as-you-go environment

Automate testing as much as possible, making each test repeatable and enabling a consistent approach to evaluating results. If reports and dashboards are inconsistent, then having the ability to compare metadata lineage across original and migrated systems is valuable during migration testing, since it can highlight differences and pinpoint where they occurred when these are not easy to detect.

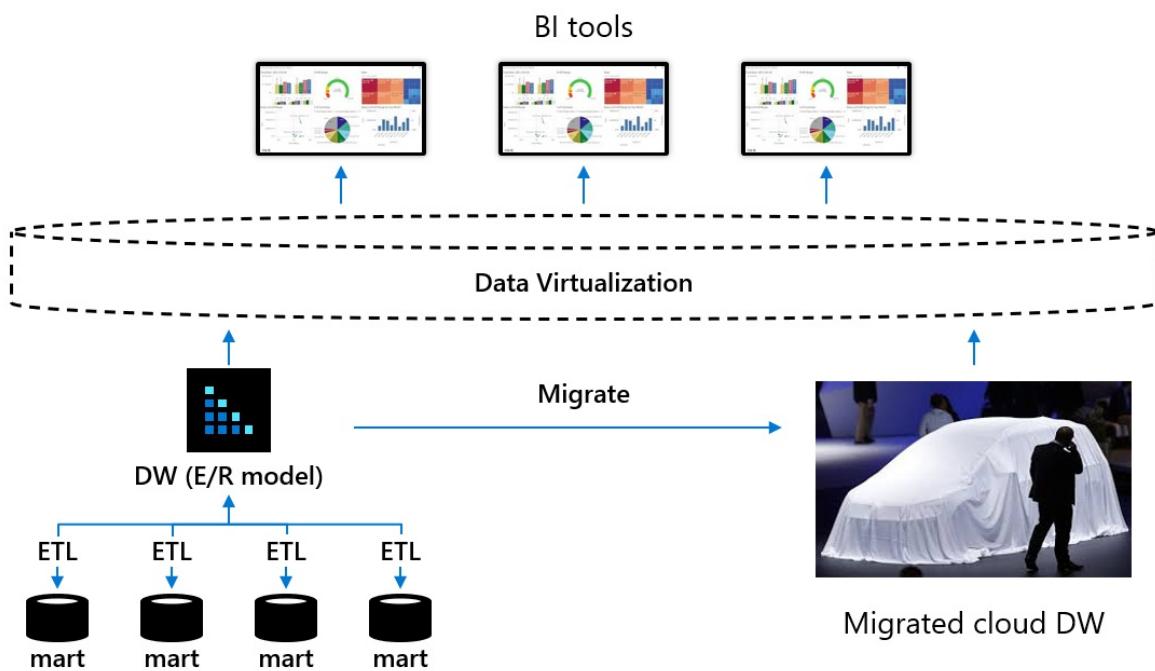
The best way to do this securely is to create roles, assign access privileges to roles and then attach users to roles. To access your newly migrated data warehouse, set up an automated process to create new users and assign roles. Do the same to remove users from roles.

Communicate the cutover to all users so they know what's changing and what to expect.

# De-risking your data warehouse migration project

Another critical factor in data warehouse migration is de-risking the project in order to maximize the likelihood of a success. There are several things that can be done to de-risk a data warehouse migration. They include:

- Establishing a proof-of-concept lab to enable your team to try things, conduct tests, understand any issues and identify fixes and optimizations that help validate migration approaches, improve performance and lower costs. It also helps establish ways to automate tasks, use built-in tools and build templates to capture best practices, learn from experience, and track lessons learned. It's an invaluable way to mitigate risk and increase your chances of success. In addition, you can assign owners to tests who are accountable for achieving migration goals and targets as defined in your migration strategy.
- Introduce data virtualization between BI tools and your data warehouse and data marts. Introduce user transparency using data virtualization to reduce risk in a data warehouse migration, and hide the migration from users by using data virtualization BI tools, as shown in the following diagram.



The purpose of this is to break the dependency between business users utilizing self-service BI tools and the physical schema of the underlying data warehouse and data marts that are being migrated. By introducing data virtualization, any schema alterations made during data warehouse and data mart migration to Azure Synapse (for example, to optimize performance) can be hidden from business users because they only access virtual tables in the data virtualization layer. If structural change is needed, only the mappings between the data warehouse or data marts and any virtual tables would need to be changed so that users remain unaware of those changes and unaware of the migration.

- Look to archive any existing tables identified as never used prior to data warehouse migration as there is little point migrating tables that are not used. One possible way of doing this is to archive the unused data to Azure blob storage or to Azure Data Lake and create external tables in Azure Synapse to that data so that it is still online.
- Consider the possibility of introducing a virtual machine (VM) on Azure with a development version (usually free) of the existing legacy data warehouse DBMS running on this VM. This allows you to quickly move existing data warehouse schema to the VM and then move it on into Azure Synapse while working entirely on the Azure cloud.
- Define migration order and dependencies.
- Ensure your infrastructure and operations teams are ready for the migration of your data as early as possible into the migration project.

- Identify the differences in DBMS functionality and where proprietary business logic could become a problem. For example, using stored procedures for ELT processing is unlikely to migrate easily and won't contain any metadata lineage since the transformations are buried in code.
- Considering a strategy to migrate data marts first followed by the data warehouse that is the source to the data marts. The reason for this is that it enables incremental migration, it makes it more manageable and it is possible to prioritize migration based on business needs.
- Considering the possibility of using data virtualization to simplify your current data warehouse architecture before you migrate, for example, to replace data marts with virtual data marts so that you can eliminate physical data stores and ETL jobs for data marts without losing any functionality prior to migration. Doing this would reduce the number of data stores to migrate, reduce copies of data, reduce the total cost of ownership and improve agility. This requires switching from physical to virtual data marts before migrating your data warehouse. In many ways, you could consider this a data warehouse modernization step prior to migration.

## Next steps

For more information on data warehouse migrations, attend a virtual [Cloud Data Warehouse Modernization Workshop on Azure](#) from Informatica.

# Ensure the environment is prepared for the cloud adoption plan

11/9/2020 • 2 minutes to read • [Edit Online](#)

Before adoption can begin, you must create a landing zone to host the workloads that you plan to build in or migrate to the cloud . This section of the framework guides you through how a landing zone is created.

The following exercises help guide you through the process of creating a landing zone to support cloud adoption.

1	<p><a href="#">Azure setup guide</a>: Review the Azure setup guide to become familiar with the tools and approaches you need to use to create a landing zone.</p>
2	<p><a href="#">Azure landing zones</a>: Choose the most appropriate landing zone option, to establish a code-based starting point for your environment.</p>
3	<p><a href="#">Expand the landing zone</a>: Meet the platform requirements of your cloud adoption plan by expanding the first landing zone.</p>
4	<p><a href="#">Best practices</a>: Validate landing zone modifications against best practices to ensure the proper configuration of your current and future landing zones.</p>

At a minimum, to get ready for cloud adoption, review the [Azure setup guide](#).

# Azure setup guide overview

11/9/2020 • 2 minutes to read • [Edit Online](#)

## NOTE

This guide provides a starting point for readiness guidance in the Cloud Adoption Framework and is also available in the Azure Quickstart Center. See the tip in the article for a link.

Before you start building and deploying solutions using Azure services, you need to prepare your environment. In this guide, we introduce features that help you organize resources, control costs, and secure and manage your organization. For more information, best practices, and considerations related to preparing your cloud environment, see the [Cloud Adoption Framework's readiness section](#).

You'll learn how to:

- **Organize resources:** Set up a management hierarchy to consistently apply access control, policy, and compliance to groups of resources and use tagging to track related resources.
- **Manage access:** Use role-based access control to make sure that users have only the permissions they really need.
- **Manage costs and billing:** Identify your subscription type, understand how billing works, and learn how to control costs.
- **Plan for governance, security, and compliance:** Enforce and automate policies and security settings that help you follow applicable legal requirements.
- **Use monitoring and reporting:** Get visibility across resources to find and fix problems, optimize performance, and gain insight into customer behavior.
- **Stay current with Azure:** Track product updates to enable a proactive approach to change management.

## TIP

For an interactive experience, view this guide in the Azure portal. Go to the [Azure Quickstart Center](#) in the Azure portal, select **Azure Setup Guide**, and then follow the step-by-step instructions.

**Next steps:**

- [Organize your resources to simplify how you apply settings](#)

This guide provides interactive steps that let you try features as they're introduced. To come back to where you left off, use the breadcrumb for navigation.

# Organize your Azure resources effectively

11/9/2020 • 6 minutes to read • [Edit Online](#)

Organizing your cloud-based resources is critical to securing, managing, and tracking the costs related to your workloads. To organize your resources, define a management group hierarchy, follow a well-considered naming convention and apply resource tagging.

- [Azure management groups and hierarchy](#)
- [Naming standards](#)
- [Resource tags](#)

Azure provides four levels of management scope: management groups, subscriptions, resource groups, and resources. The following image shows the relationship of these levels.

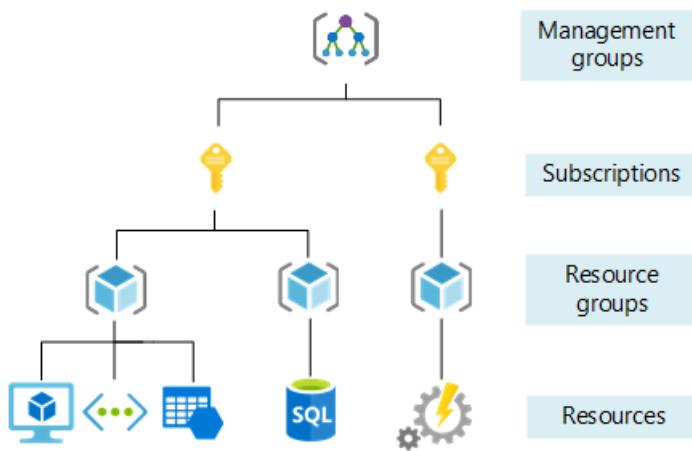


Figure 1: How the four management-scope levels

relate to each other.

- **Management groups:** These groups are containers that help you manage access, policy, and compliance for multiple subscriptions. All subscriptions in a management group automatically inherit the conditions applied to the management group.
- **Subscriptions:** A subscription logically associates user accounts and the resources that were created by those user accounts. Each subscription has limits or quotas on the amount of resources you can create and use. Organizations can use subscriptions to manage costs and the resources that are created by users, teams, or projects.
- **Resource groups:** A resource group is a logical container into which Azure resources like web apps, databases, and storage accounts are deployed and managed.
- **Resources:** Resources are instances of services that you create, like virtual machines, storage, or SQL databases.

## Scope of management settings

You can apply management settings like policies and role-based access control at any of the management levels. The level you select determines how widely the setting is applied. Lower levels inherit settings from higher levels. For example, when you apply a policy to a subscription, that policy is also applied to all resource groups and resources in that subscription.

Usually, it makes sense to apply critical settings at higher levels and project-specific requirements at lower levels. For example, you might want to make sure all resources for your organization are deployed to certain regions. To do that, apply a policy to the subscription that specifies the allowed locations. As other users in your organization add new resource groups and resources, the allowed locations are automatically enforced. Learn more about policies in the governance, security, and compliance section of this guide.

If you have only a few subscriptions, it's relatively simple to manage them independently. If the number of subscriptions you use increases, consider creating a management group hierarchy to simplify the management of your subscriptions and resources. For more information, see [Organize and manage your Azure subscriptions](#).

As you plan your compliance strategy, work with people in your organization with these roles: security and compliance, IT administration, enterprise architecture, networking, finance, and procurement.

## Create a management level

You can create a management group, additional subscriptions, or resource groups.

### Create a management group

Create a management group to help you manage access, policy, and compliance for multiple subscriptions.

1. Go to [management groups](#).
2. Select **Add management group**.

### Create a subscription

Use subscriptions to manage costs and resources that are created by users, teams, or projects.

1. Go to [subscriptions](#).
2. Select **Add**.

#### NOTE

Subscriptions can also be created programmatically. For more information, see [Programmatically create Azure subscriptions](#).

### Create a resource group

Create a resource group to hold resources like web apps, databases, and storage accounts that share the same lifecycle, permissions, and policies.

1. Go to [resource groups](#).
2. Select **Add**.
3. Select the **Subscription** that you want your resource group created under.
4. Enter a name for the **Resource group**.
5. Select a **Region** for the resource group location.

## Learn more

To learn more, see:

- [Azure fundamentals](#)
- [Create your initial subscriptions](#)
- [Create additional Azure subscriptions to scale your Azure environment](#)
- [Organize and manage your Azure subscriptions](#)
- [Organize your resources with Azure management groups](#)
- [Understand resource access management in Azure](#)
- [Subscription service limits](#)

## Actions

### Create a management group:

Create a management group to help you manage access, policy, and compliance for multiple subscriptions.

1. Go to **Management groups**.
2. Select **Add management group**.

GO TO MANAGEMENT  
GROUPS

### Create an additional subscription:

Use subscriptions to manage costs and resources that are created by users, teams, or projects.

1. Go to **Subscriptions**.
2. Select **Add**.

GO TO  
SUBSCRIPTIONS

### Create a resource group:

Create a resource group to hold resources like web apps, databases, and storage accounts that share the same lifecycle, permissions, and policies.

1. Go to **Resource groups**.
2. Select **Add**.
3. Select the **Subscription** that you want your resource group created under.
4. Enter a name for the **Resource group**.
5. Select a **Region** for the resource group location.

CREATE A RESOURCE  
GROUP

# Manage access to your Azure environment with role-based access control

11/9/2020 • 2 minutes to read • [Edit Online](#)

Managing who can access your Azure resources and subscriptions is an important part of your Azure governance strategy, and assigning group-based access rights and privileges is a good practice. Dealing with groups rather than individual users simplifies maintenance of access policies, provides consistent access management across teams, and reduces configuration errors. Azure role-based access control (RBAC) is the primary method of managing access in Azure.

RBAC provides detailed access management of resources in Azure. It helps you manage who has access to Azure resources, what they can do with those resources, and what scopes they can access.

When you plan your access control strategy, grant users the least privilege required to get their work done. The following image shows a suggested pattern for assigning RBAC.

	Role			
	Reader	Resource-specific or custom role	Contributor	Owner
Subscription	Observers			
Resource group		Users managing resources		Admins
Resource			Automated processes	

Figure 1: RBAC

roles.

When you plan your access control methodology, we recommend that you work with people in your organizations with the following roles: security and compliance, IT administration, and enterprise architect.

The Cloud Adoption Framework offers additional guidance on using [role-based access control](#) in your cloud adoption efforts.

## Actions

### Grant resource group access:

To grant a user access to a resource group:

1. Go to [Resource groups](#).
2. Select a resource group.
3. Select [Access control \(IAM\)](#).
4. Select + Add > Add role assignment.
5. Select a role, and then assign access to a user, group, or service principal.

GO TO RESOURCE  
GROUPS

## Grant subscription access:

To grant a user access to a subscription:

1. Go to **Subscriptions**.
2. Select a subscription.
3. Select **Access control (IAM)**.
4. Select + Add > **Add role assignment**.
5. Select a role, and then assign access to a user, group, or service principal.



## Grant resource group access

To grant a user access to a resource group:

1. Go to [resource groups](#).
2. Select a resource group.
3. Select **Access control (IAM)**.
4. Select + Add > **Add role assignment**.
5. Select a role, and then assign access to a user, group, or service principal.

## Grant subscription access

To grant a user access to a subscription:

1. Go to [subscriptions](#).
2. Select a subscription.
3. Select **Access control (IAM)**.
4. Select + Add > **Add role assignment**.
5. Select a role, and then assign access to a user, group, or service principal.

## Learn more

To learn more, see:

- [What is role-based access control \(Azure RBAC\)?](#)
- [Cloud Adoption Framework: Use role-based access control](#)

# Manage costs and billing for your Azure resources

11/9/2020 • 2 minutes to read • [Edit Online](#)

Cost management is the process of effectively planning and controlling costs involved in your business. Cost management tasks are typically performed by finance, management, and app teams. Azure Cost Management and Billing can help you plan with cost in mind. It can also help you to analyze costs effectively and take action to optimize cloud spending.

For more information about integrating cloud cost management processes throughout your organization, see the Cloud Adoption Framework article on how to [track costs across business units, environments, or projects](#).

## Manage your costs with Azure Cost Management and Billing

Azure Cost Management and Billing provides a few ways to help you predict and manage costs:

- **Analyze cloud costs** helps you explore and analyze your costs. You can view aggregated cost for your account or view accumulated costs over time.
- **Monitor with budgets** allows you to create a budget and then configure alerts to warn you when you're close to exceeding it.
- **Optimize with recommendations** helps identify idle and underused resources so you can take action to reduce waste.
- **Manage invoices and payments** gives you visibility to your cloud investment.

### Predict and manage costs

1. Go to [Cost Management + Billing](#).
2. Select **Cost Management**.
3. Explore the features that help to analyze and optimize cloud costs.

### Manage invoices and payment methods

1. Go to [Cost Management + Billing](#).
2. Select **Invoices** or **Payment methods** from the **Billing** section in the left pane.

## Billing and subscription support

We offer 24-hour access every day for billing and subscription support to Azure customers. If you need assistance to understand Azure usage, create a support request.

### Create a support request

To submit a new support request:

1. Go to [help + support](#).
2. Select **New support request**.

### View a support request

To view your support requests and their status:

1. Go to [help + support](#).
2. Select **All support requests**.

## Learn more

To learn more, see:

- [Azure cost management and billing documentation](#)
- [Cloud Adoption Framework: Track costs across business units, environments, or projects](#)
- [Cloud Adoption Framework: Cost Management discipline](#)

## Actions

**Predict and manage costs:**

1. Go to **Cost Management + Billing**.
2. Select **Cost Management**.

**Manage invoices and payment methods:**

1. Go to **Cost Management + Billing**.
2. Select **Invoices** or **Payment methods** from the **Billing** section in the left pane.



**Billing and subscription support:**

We offer 24-hour access every day for billing and subscription support to Azure customers. If you need assistance to understand Azure usage, create a support request.

**Create a support request:**

To submit a new support request:

1. Go to **Help + Support**.
2. Select **New support request**.

**View a support request:** To view your support requests and their status:

1. Go to **Help + Support**.
2. Select **All support requests**.



# Governance, security, and compliance in Azure

11/9/2020 • 3 minutes to read • [Edit Online](#)

As you establish corporate policy and plan your governance strategies, you can use tools and services like Azure Policy, Azure Blueprints, and Azure Security Center to enforce and automate your organization's governance decisions. Before you start your governance planning, use the [governance benchmark tool](#) to identify potential gaps in your organization's cloud governance approach. For more information about developing governance processes, see the [Govern methodology](#).

- [Azure Blueprints](#)
- [Azure Policy](#)
- [Azure Security Center](#)

Azure Blueprints enables cloud architects and central information technology groups to define a repeatable set of Azure resources that implements and adheres to an organization's standards, patterns, and requirements. Azure Blueprints makes it possible for development teams to rapidly build and stand up new environments and trust that they're building within organizational compliance using a set of built-in components like networking to speed up development and delivery.

Blueprints are a declarative way to orchestrate the deployment of various resource templates and other artifacts like:

- Role assignments.
- Policy assignments.
- Azure Resource Manager templates.
- Resource groups.

## Create a blueprint

To create a blueprint:

1. Go to [Blueprints: Getting started](#).
2. In the **Create a Blueprint** section, select **Create**.
3. Filter the list of blueprints to select the appropriate blueprint.
4. Enter the **Blueprint name**, then select the appropriate **Definition location**.
5. Select **Next : Artifacts >>**, Then review the artifacts included in the blueprint.
6. Select **Save Draft**.



1. In the Azure portal, go to [Blueprints: Get started](#).
2. In the **Create a Blueprint** section, select **Create**.
3. Filter the list of blueprints to select the appropriate blueprint.
4. Enter the **Blueprint name**, then select the appropriate **Definition location**.
5. Select **Next : Artifacts >>**, Then review the artifacts included in the blueprint.
6. Select **Save Draft**.

## Publish a blueprint

To publish a blueprint artifacts to your subscription:

1. Go to [Blueprints: Blueprint definitions](#).

2. Select the blueprint you created in the previous steps.
3. Review the blueprint definition , then select **Publish blueprint**.
4. Provide a **Version** (such as *1.0*) and any **Change notes**, then select **Publish**.



1. In the Azure portal, go to [Blueprints: Blueprint definitions](#).
2. Select the blueprint definition you created in the previous steps.
3. Review the blueprint definition, then select **Publish blueprint**.
4. Provide a **Version** (such as *1.0*) and any **Change notes**, then select **Publish**.

## Learn more

To learn more, see:

- [Azure Blueprints](#)
- [Cloud Adoption Framework: Resource consistency decision guide](#)
- [Standards-based blueprints samples](#)

# Monitoring and reporting in Azure

11/9/2020 • 4 minutes to read • [Edit Online](#)

Azure offers many services that together provide a comprehensive solution for collecting, analyzing, and acting on telemetry from your applications and the Azure resources that support them. In addition, these services can extend to monitoring critical on-premises resources to provide a hybrid monitoring environment.

- [Azure Monitor](#)
- [Azure Service Health](#)
- [Azure Advisor](#)
- [Azure Security Center](#)

Azure Monitor provides a single unified hub for all monitoring and diagnostics data in Azure. You can use it to get visibility across your resources. With Azure Monitor, you can find and fix problems and optimize performance. You also can understand customer behavior.

- **Monitor and visualize metrics.** Metrics are numerical values available from Azure resources that help you understand the health of your systems. Customize charts for your dashboards, and use workbooks for reporting.
- **Query and analyze logs.** Logs include activity logs and diagnostic logs from Azure. Collect additional logs from other monitoring and management solutions for your cloud or on-premises resources. Log Analytics provides a central repository to aggregate all this data. From there, you can run queries to help troubleshoot issues or to visualize data.
- **Set up alerts and actions.** Alerts proactively notify you of critical conditions. Corrective actions can be taken based on triggers from metrics, logs, or service health issues. You can set up different notifications and actions and send data to your IT service management tools.

Start monitoring your:

- [Applications](#)
- [Containers](#)
- [Virtual machines](#)
- [Networks](#)

To monitor other resources, find additional solutions in the Azure Marketplace.

To explore Azure Monitor, go to the [Azure portal](#).

## Learn more

To learn more, see [Azure Monitor documentation](#).

## Action

[EXPLORE AZURE](#)  
[MONITOR](#)

# Stay current with Azure

11/9/2020 • 2 minutes to read • [Edit Online](#)

Cloud platforms like Azure change faster than many organizations are accustomed to. This pace of change means that organizations have to adapt people and processes to a new cadence. If you're responsible for helping your organization keep up with change, you might feel overwhelmed at times. The resources listed in this section can help you stay up to date.

- [Top resources](#)
- [Additional resources](#)

The following resources can help you stay current with Azure:

- **Azure Service Health:** [Service Health](#) alerts provide timely notifications about ongoing service issues, planned maintenance, and health advisories. These alerts also includes information about Azure features scheduled for retirement.
- **Azure updates:** Review [Azure updates](#) for announcements about product updates. Brief summaries link to additional details, making the updates easy to follow. Subscribe via the [Azure updates RSS feed](#).
- **Azure blog:** The [Azure blog](#)communicates the most important announcements for the Azure platform. Follow this blog to stay up to date on critical information. Subscribe via the [Azure blog RSS feed](#).
- **Service-specific blogs:** Many individual Azure services publish blogs that you can follow if you rely on those services. Find the ones you're interested in via a web search.
- **Azure Info Hub:** The unofficial [Azure Info Hub](#) pulls together most of the resources listed here. Follow links to individual services to get detailed information and find service-specific blogs. Subscribe via [the Azure Info Hub RSS feed](#). \*

# Understand cloud operating models

11/9/2020 • 3 minutes to read • [Edit Online](#)

Adopting the cloud creates an opportunity to revisit how you operate technology systems. This article series will clarify cloud operating models and the considerations that impact your cloud adoption strategy. But first, let's clarify the term *cloud operating model*.

## Define your operating model

Before deploying your cloud architecture, it's important to understand how you want to operate in the cloud. Understanding your strategic direction, people organization, and governance, risk, and compliance (GRC) needs helps define your future state cloud operating model. Then, Azure landing zones can provide a variety of architecture and implementation options to support your operating model. The next few articles will share a few foundational terms and provide examples of common operating models based on actual customer experiences, which together can guide your decision about the right Azure landing zone to implement.

## What is an operating model?

Prior to the existence of cloud technologies, technology teams established operating models to define how technology would support the business. Any company's IT operating model has a number of factors, but a few remain consistent: *alignment to business strategy, organization of people, change management (or adoption processes), operations management, governance/compliance, and security*. Each factor is essential to long-term technology operations.

When technology operations shift to the cloud, these vital processes are still relevant, but they're likely to change in some ways. Current operating models focus heavily on physical assets in physical locations funded largely through capital expenditure cycles. These assets are used to support the workloads that the business needs to maintain business operations. The mission of most operating models is to prioritize stability of the workloads by investing in the stability of the underlying physical assets.

## How is a cloud operating model different?

Redundancy in the hardware stack is a never-ending cycle. Physical hardware breaks down. Performance degrades. The degradation of hardware rarely aligns with the predictable budgetary cycles of an organization's capital expenditure planning cycles. Operating in the cloud breaks the treadmill of hardware refreshes and midnight patches by shifting the focus upstream to the digital assets: operating systems, applications, and data. This shift from physical to digital also shifts the technology operating model.

As your operating model shifts to the cloud, you still need the same people and processes, but they also shift to focus on a higher level of operations. If your people no longer focus on server uptime, then their success metrics will change. If security is no longer protected by the four walls of a datacenter, then your threat profile changes. When procurement is no longer a blocker to innovation, then the pace at which you manage change also changes.

A *cloud operating model* is the collection of processes and procedures that define how you want to operate technology in the cloud.

## Purpose of a cloud operating model

When hardware is removed as the most common unit of operations, the focus shifts to the digital assets and the workloads they support. As such, the purpose of the operating model shifts from keeping the lights on to ensuring consistent operations.

The [Microsoft Azure Well-Architected Framework](#) does a great job of decomposing workload considerations into a set of common architectural principles: cost optimization, operational excellence, performance efficiency, reliability, and security.

When moving to a higher level of operations, these common architectural principles help reframe the purpose of the cloud operating model. How do we ensure that all assets and workloads in the portfolio balance these architecture principles? What processes are needed to scale the application of those principles?

## Reimagine your operating model

If you updated your operating model to remove every reference to the procurement, change, operations, or protection of physical assets, what's left? For some organizations, their operating model is now a clean slate. For most organizations, the constraints that have developed over the years are now reduced. In either case, there is an opportunity to think about how you would like to operate in the cloud.

To help you imagine your future state operating model, these articles discuss the following subjects:

- [Define your cloud operating model](#)
- [Compare common cloud operating models](#)
- [Implement your operating model with Azure landing zones](#)

## Next steps

Learn how the Cloud Adoption Framework helps you define your operating model.

[Compare common cloud operating models](#)

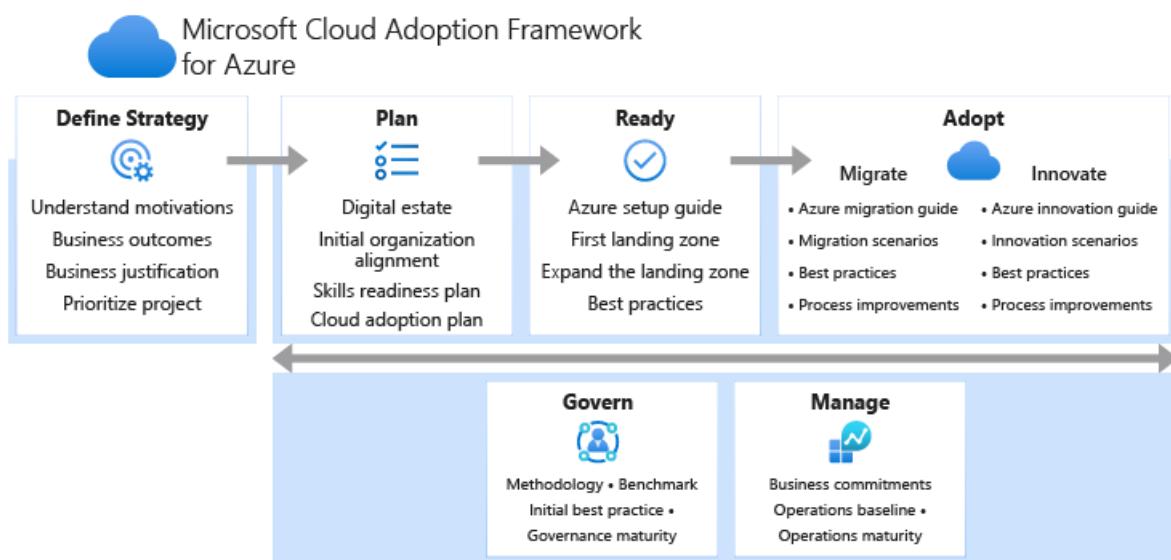
# Define your cloud operating model

11/9/2020 • 2 minutes to read • [Edit Online](#)

Cloud operating models are complex. Countless customers become blocked by minor details while defining their cloud operating model. It's easy to fall into a series of circular references. To avoid circular references, the Cloud Adoption Framework provides a series of complimentary and incremental methodologies that decompose the volume of decisions into smaller exercises.

## Cloud Adoption Framework alignment

To help you define the cloud operating model for your business, the Cloud Adoption Framework breaks down each aspect of the operating model into methodologies. Each methodology and the associated actionable exercises are designed to help you define your future state operations.



### Support to develop your operating model

The following areas of the Cloud Adoption Framework are incremental methodologies designed to help grow areas of your operating model.

- **Manage**: Align ongoing processes for operational management of the technology to maximize value attainment and minimize disruptions.
- **Govern**: Ensure consistency across adoption efforts. Align to governance or compliance requirements to maintain a cross-cloud environment.
- **Security strategy**: Help for defining your overall security strategy.
- **Organize**: Outlines the functions needed in the cloud. Also defines ways to organize people and align responsibilities.

### Collective output of the operating model

Your environment should represent how you want to operate. As you define your operating model, environmental readiness should match your operations, governance, security, and organizational requirements.

- **Ready**: Azure landing zones provide deployment guidance and reference implementations to act on operating model decisions in the form of environmental configuration.

#### **NOTE**

The Ready methodology provides several implementation options to Azure landing zones:

- **Start small and expand:** Designed to build your cloud platform as you define each aspect of your operating model.
- **Enterprise-scale:** Build out an enterprise ready architecture based on a set of defined operating-model decisions.

### **Dependencies and inputs to operating model decisions**

The business strategy and collective cloud adoption plans are inputs that should be considered when defining your operating model.

- **Strategy:** Guidance to capture business strategy and map those to efforts that can be enabled by a cloud adoption strategy.
- **Plan:** Agile-based change management guidance to establish backlogs and align ongoing change.

## **Next steps**

Before engaging any of the above methodologies, use the next article to compare common cloud operating models and find a model that closely matches your requirements. That article will help establish the most actionable starting point and set of exercises to move you towards the desired operating model across your cloud platform.

[Compare common cloud operating models](#)

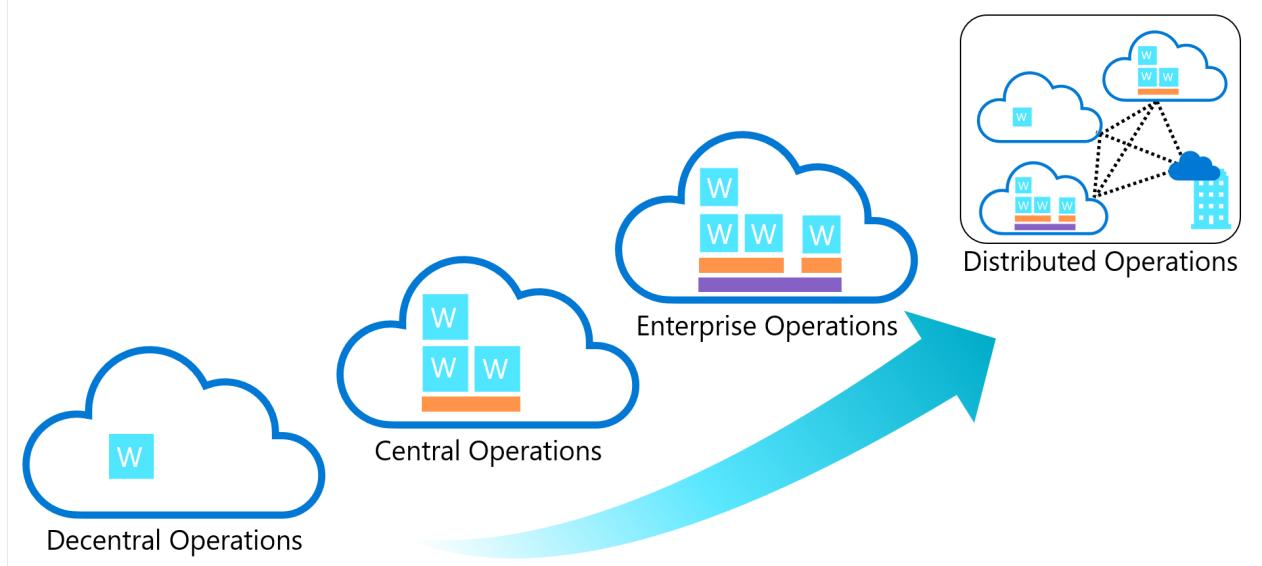
# Compare common cloud operating models

11/9/2020 • 21 minutes to read • [Edit Online](#)

Operating models are unique and specific to the business they support, based on their current requirements and constraints. But, this uniqueness shouldn't suggest that operating models are *snowflakes*. There are a few common patterns of customer operating models. This article outlines the four most common patterns.

## Operating model comparison

The following image maps common operating models based on the range of complexity, from least complex (decentralized) to most complex (global operations). The tables below compares the same operating models based on relative value of a few other attributes.



### Priorities or scope

A cloud operating model is primarily driven by two factors:

- Strategic priorities and motivations.
- The scope of the portfolio to be managed.

	DECENTRALIZED OPERATIONS (OPS)	CENTRALIZED OPERATIONS (OPS)	ENTERPRISE OPERATIONS (OPS)	DISTRIBUTED OPERATIONS (OPS)
Strategic priority	Innovation	Control	Democratization	Integration
Portfolio scope	Workload	Landing zone	Cloud platform	Full portfolio
Workload environment	High complexity	Low complexity	Medium complexity	Medium or variable complexity
Landing zone	N/A	High complexity	Medium to low complexity	Low complexity

	DECENTRALIZED OPERATIONS (OPS)	CENTRALIZED OPERATIONS (OPS)	ENTERPRISE OPERATIONS (OPS)	DISTRIBUTED OPERATIONS (OPS)
Foundation utilities	N/A	N/A or low support	Centralized and more support	Most support
Cloud foundation	N/A	N/A	Hybrid, provider specific, or regional foundations	Distributed and synchronized

- **Strategic priorities or motivations:** Each operating model is capable of delivering the typical [strategic motivations for cloud adoption](#). However, some operating models simplify realizing specific motivations.
- **Portfolio scope:** The portfolio scope row below identifies the largest scope that a specific operating model is designed to support. For example, centralized operations is designed for a small number of landing zones. But that operating model decision could inject operational risks for an organization that's trying to manage a large, complex portfolio that might require many landing zones or variable complexity in landing zone design.

#### IMPORTANT

Adopting the cloud often triggers a reflection on the current operating model and might lead to a shift from one of the common operating models to another. But cloud adoption isn't the only trigger. As business priorities and the scope of cloud adoption change how the portfolio needs to be supported, there could be other shifts in the most-appropriately aligned operating model. When the board or other executive teams develop 5 to 10 year business plans, those plans often include a requirement (explicit or implied) to adjust the operating model. While these common models are a good reference for guiding decisions, keep in mind that your operating model might change or you might need to customize one of these models to meet your requirements and constraints.

#### Accountability alignment

While many teams and individuals will be responsible for supporting different functions, each of the common operating models assigns final accountability for decisions and their outcomes to one team or one individual. This approach affects how the operating model is funded and what level of support is provided for each function.

	DECENTRALIZED OPS	CENTRALIZED OPS	ENTERPRISE OPS	DISTRIBUTED OPS
Business alignment	Workload team	Central cloud strategy	CCoE	Variable - <a href="#">form a broad cloud strategy team?</a>
Cloud operations	Workload team	Central IT	CCoE	Based on portfolio analysis - see <a href="#">Business alignment</a> and <a href="#">business commitments</a>
Cloud governance	Workload team	Central IT	CCoE	Multiple layers of governance
Cloud security	Workload team	Security operations center (SOC)	CCoE + SOC	Mixed - see <a href="#">Define a security strategy</a>

	DECENTRALIZED OPS	CENTRALIZED OPS	ENTERPRISE OPS	DISTRIBUTED OPS
Cloud automation and DevOps	Workload team	Central IT or N/A	CCoE	Based on portfolio analysis - see <a href="#">Business alignment and business commitments</a>

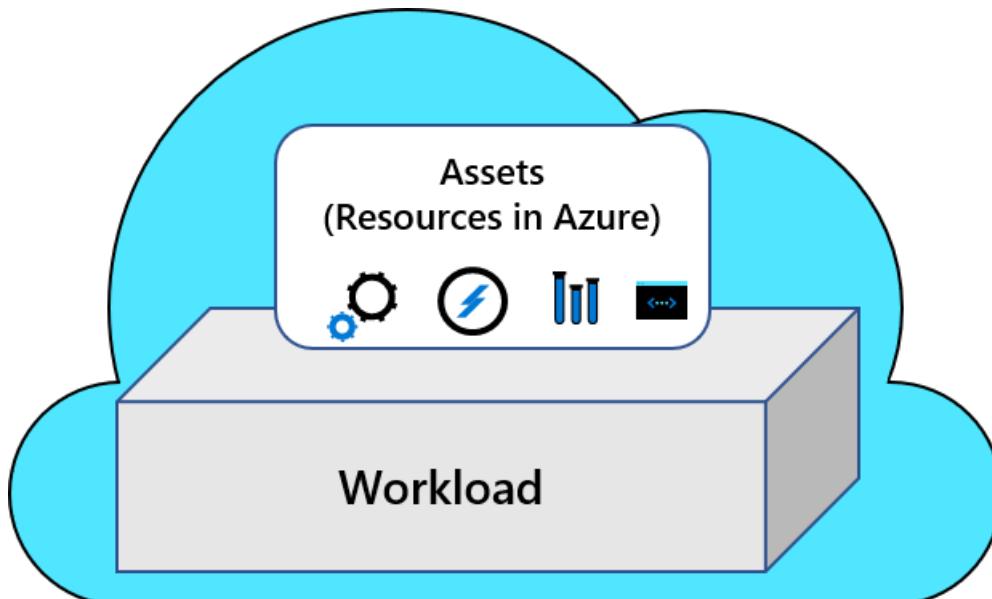
### Accelerate operating model implementation in Azure

As discussed in [Define your operating model](#), each methodology of the Cloud Adoption Framework provides a structured path to iteratively developing each aspect of your operating model. Following the most relevant methodology will help you overcome blockers to adoption that stem from gaps in the cloud operating model.

But there are ways to accelerate your operating model implementation, as outlined in the table below.

	DECENTRALIZED OPS	CENTRALIZED OPS	ENTERPRISE OPS	DISTRIBUTED OPS
Starting point	Azure Well-Architected Framework (WAF)	Azure landing zones: <a href="#">start-small options</a>	Azure landing zones: <a href="#">CAF enterprise-scale</a>	<a href="#">Business alignment</a>
Iterations	A focus on workloads allows the team to iterate within WAF.	The start-small option requires additional iteration on each methodology, but that can be done as cloud adoption efforts mature.	As illustrated by the reference implementations, future iterations typically focus on minor configuration additions.	Review the <a href="#">Azure landing zone implementation options</a> to start with the option that best meets your operations baseline. Follow the iteration path defined in that option's design principles.

## Decentralized operations



Operations is always complex. By limiting the scope of operations to one workload or a small collection of workloads, that complexity can be controlled. As such, decentralized operations is the least complex of the common operating models. In this form of operations, all workloads are operated independently by dedicated workload teams.

- **Priorities:** Innovation is prioritized over centralized control or standardization across multiple workloads.
- **Distinct advantage:** Maximizes speed of innovation by placing workload and business teams in full control of design, build, and operations.
- **Distinct disadvantage:** Reduction in cross-workload standardization, economies of scale through shared services, and consistent governance centralized compliance efforts.
- **Risk:** This approach introduces risk when managing a portfolio of workloads. Since the workload team is less likely to have specialized teams dedicated to central IT functions, this operating model is viewed as a high risk option by some organizations, especially companies that are required to follow third-party compliance requirements.
- **Guidance:** Decentralized operations are limited to workload level decisions. The Microsoft Azure Well-Architected Framework is designed to support the decisions made within that scope. The processes and guidance within the Cloud Adoption Framework are likely to add overhead that are not required by decentralized operations.

### **Advantages of decentralized operations**

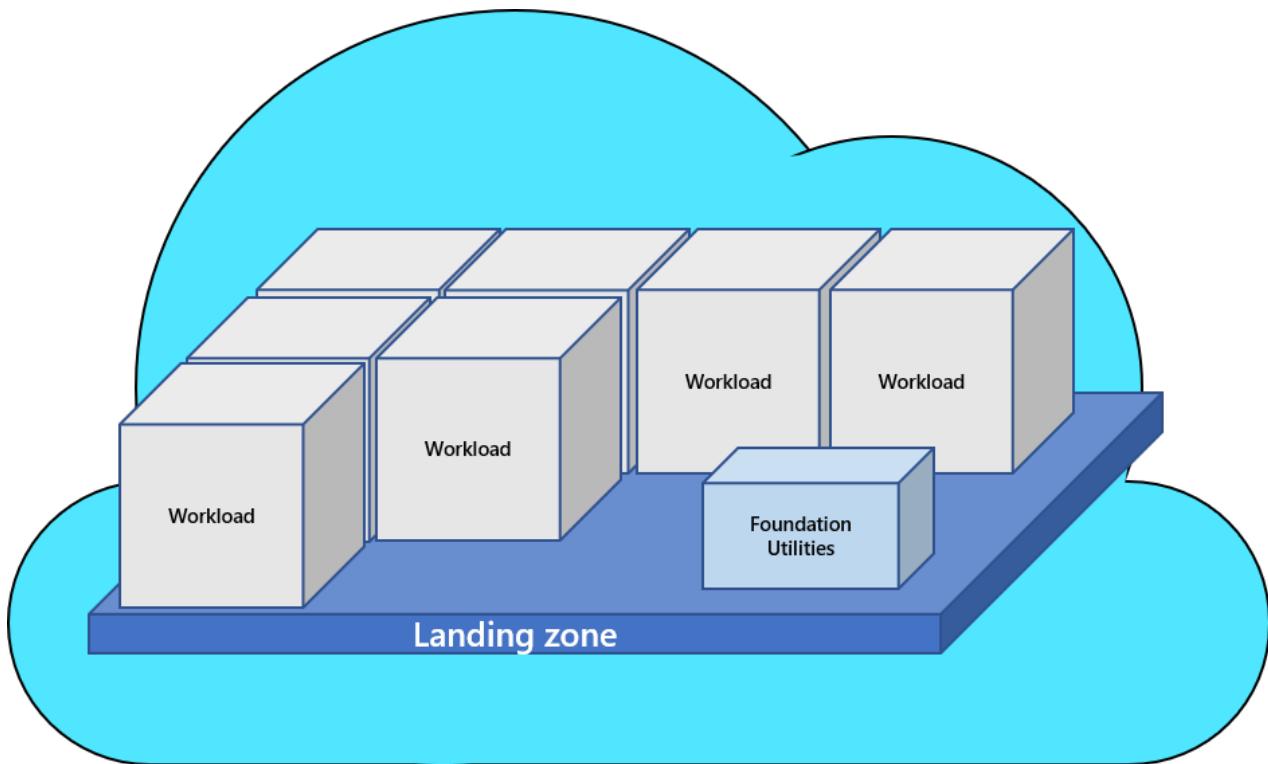
- **Cost management:** Cost of operations can be easily mapped to a single business unit. Workload-specific operations allow for greater workload optimization.
- **Responsibilities:** Typically, this form of operations is highly dependent on automation to minimize overhead. Responsibilities tend to focus on DevOps and pipelines for release management. This allows for faster deployments and shorter feedback cycles during development.
- **Standardization:** Source code and deployment pipeline should be used to standardize the environment from release to release.
- **Operations support:** Decisions that impact operations are only concerned with the needs of that workload, simplifying operations decisions. Many in the DevOps community would argue that this is the purest form of operations because of the tighter operational scope.
- **Expertise:** DevOps and development teams are most empowered by this approach and experience the least resistance to driving market change.
- **Landing zone design:** No specific operational advantage.
- **Foundational utilities:** No specific operational advantage.
- **Separation of duties:** No specific operational advantage.

### **Disadvantages of decentralized operations**

- **Cost management:** Enterprise costs are harder to calculate. Lack of centralized governance teams make it harder to implement uniform cost controls or optimization. At scale, this model can be costly, since each workload would likely have duplication in deployed assets and staffing assignments.
- **Responsibilities:** Lack of centralized supporting teams means that the workload team is entirely responsible for governance, security, operations, and change management. This is a detriment when those tasks have not been automated in code review and release pipelines.
- **Standardization:** Standardization across a portfolio of workloads can become variable and inconsistent.
- **Operations support:** Scale efficiencies are often missed. As our uniform best practices across multiple workloads.
- **Expertise:** Team members have a greater responsibility to make wise and ethical decisions regarding governance, security, operations, and change management decisions within the application design and configuration. The Microsoft Azure Well-Architected Review and Azure Well-Architected Framework should be consulted frequently to improve the required expertise.
- **Landing zone design:** Landing zones are not workload-specific and are not considered in this approach.
- **Foundational utilities:** Few (if any) foundational services are shared across workloads, reducing scale efficiencies.
- **Separation of duties:** Higher requirements for DevOps and development teams increase the usage of elevated privileges from those teams. If separation of duties is required, heavy investment in DevOps maturity

will be needed to operate in this approach.

## Centralized operations



Stable state environments might not require as much focus on the architecture or distinct operational requirements of the individual workloads. Central operations tend to be the norm for technology environments that consist primarily of stable-state workloads. Examples of a stable-state of operations include things like commercial-off-the-shelf (COTS) applications or well-established custom applications that have a slow release cadence. When rate of change is driven by a regular drumbeat of updates and patches (over the high change rate of innovation), centralization of operations is an effective means to manage the portfolio.

- **Priorities:** Prioritizes central control over innovation. Also prioritizes continuation of existing operational processes over cultural shift to modern cloud operations options.
- **Distinct advantage:** Centralization introduces economies of scale, best-of-breed controls, and standardized operations. This approach works best with the cloud environment needs specific configurations integrate cloud operations into existing operations and processes. This approach is most advantageous to centralized teams with a portfolio of a few hundred workloads with modest architectural complexity and compliance requirements.
- **Distinct disadvantage:** Scaling to meet the demands of a large portfolio of workloads can place significant strain on a centralized team making operational decisions for production workloads. If technical assets are expected to scale beyond 1,000 or so VMs, applications, or data sources in the cloud within the next 18-24 months, an enterprise model should be considered.
- **Risk:** This approach limits centralization to a smaller number of subscriptions (often one production subscription). There is a risk of significant refactoring later in the cloud journey that could interfere with adoption plans. Specifically, care should be given to segmentation, environment boundaries, identity tooling, and other foundational elements to avoid significant rework in the future.
- **Guidance:** Azure landing zone implementation options aligned to the "start small and expand" development velocity creates a sound starting point. Those can be used to accelerate adoption efforts. To be successful, clear policies must be established to guide early adoption efforts within acceptable risk tolerances. Govern and Manage methodologies create processes to mature operations in parallel. Those steps serve as stage gates that must be completed before allowing for increased risk as operations matures.

### Advantages of centralized operations

- **Cost management:** Centralizing shared services across a number of workloads creates economies of scale and eliminates duplicated tasks. Central teams can more quickly implement cost reductions through enterprise-wide sizing and scale optimizations.
- **Responsibilities:** Centralized expertise and standardization is likely to lead to higher stability, better operational performance, and lower risk of change-related outages. This reduces broad skilling pressures on the workload focused teams.
- **Standardization:** In general, standardization and cost of operations is lowest with a centralized model because there are fewer duplicated systems or tasks.
- **Operations support:** Reducing complexity and centralizing operations makes it easy for smaller IT teams to support operations.
- **Expertise:** Centralization of supporting teams allow for experts in the fields of security, risk, governance, and operations to drive business critical decisions.
- **Landing zone design:** Central IT tends to minimize the number of landing zones and subscriptions to reduce complexity. Landing zone designs tend to mimic the preceding datacenter designs, which reduces transition time. As adoption progresses, shared resources can then be moved out into a separate subscription or platform foundation.
- **Foundational utilities:** Carrying existing datacenter designs into the cloud results in foundational, shared services that mimic on-premises tools and operations. When on-premises operations are your primary operating model, this can be an advantage (beware the disadvantages below). Doing so reduces transition time, capitalizes on economies of scale, and allows for consistent operational processes between on-premises and cloud hosted workloads. This approach can reduce short-term complexity/effort and allow smaller teams to support cloud operations with reduced learning curves.
- **Separation of duties:** Separation of duties is clear in central operations. Central IT maintains control of the production environments reducing the need for any elevated permissions from other teams. This reduces the surface area of breach by reducing the number of accounts with elevated privileges.

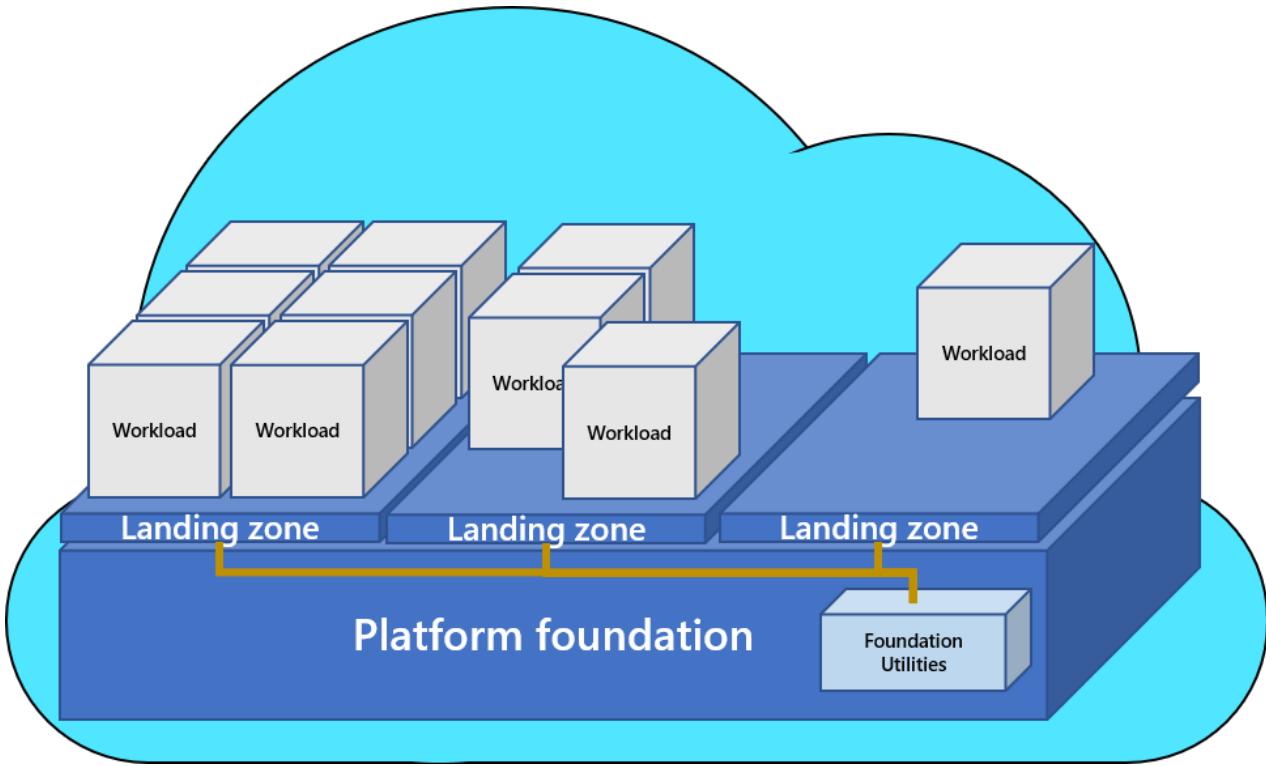
### **Disadvantages of centralized operations**

- **Cost management:** Central teams rarely have enough understanding of the workload architectures to produce impactful optimizations at the workload level. This limits the amount of cost savings that can come from well-tuned workload operations. Further, lack of workload architecture understanding can cause centralized cost optimizations to have a direct impact on performance, scale, or other pillars of a well-architected workload. Before applying enterprise-wide cost changes to high profile workloads, the Microsoft Azure Well-Architected Review should be completed and considered by the central IT team.
- **Responsibilities:** Centralizing production support and access places a higher operational burden on a smaller number of people. It also places greater pressure on those individuals to perform deeper reviews of the deployed workloads to validate adherence to detailed security, governance, and compliance requirements.
- **Standardization:** Central IT approaches make it difficult to scale standardization without a linear scaling of central IT staff.
- **Operations support:** Not the disadvantage and risks listed above. The greatest disadvantages of this approach are associated with significant scale and shifts that prioritize innovation.
- **Expertise:** Developer and DevOps experts are at risk of being under-valued or too constrained in this type of environment.
- **Landing zone design:** Datacenter designs are based on the constraints of preceding approaches, which aren't always relevant to the cloud. Following this approach reduces the opportunities to rethink environment segmentation and empower innovation opportunities. Lack of landing zone segmentation also increases the potential impact of breach, increases complexity of governance/compliance adherence, and could create blockers to adoption later in the cloud journey. See the risks section above.
- **Foundational utilities:** During digital transformation, cloud might become the primary operating model. Persisting central tools built for on-premises operations reduces opportunities to modernize operations and drive increased operational efficiencies. Choosing not to modernize operations early in the adoption process can be overcome through creation of a platform foundations subscription later in the cloud adoption journey,

but that effort can be complex, costly, and time consuming without advanced planning.

- **Separation of duties:** Central operations generally follow one of two paths, both of which can hinder innovation.
  - **Option 1:** Teams outside of central IT are granted limited access to development environments that mimic production. This option hinders experimentation.
  - **Option 2:** Teams develop and test in non-supported environments. This option hinders deployment processes and slows post-deployment integration testing.

## Enterprise operations



Enterprise operations is the suggested target state for all cloud operations. Enterprise operations balances the need for control and innovation by democratizing decisions and responsibilities. Central IT is replaced by a more facilitative cloud center of excellence or CCoE team, which supports workload teams and hold them accountable for decisions, as opposed to controlling or limiting their actions. Workload teams are granted more power and more responsibility to drive innovation, within well-defined guardrails.

- **Priorities:** Prioritizes democratization of technical decisions. Democratization of technical decisions shifts responsibilities previously held by central IT to workload teams when applicable. To deliver this shift in priorities, decisions become less dependent on human-run review processes and more dependent on automated review, governance, and enforcement using cloud-native tools.
- **Distinct advantage:** Segmentation of environments and separation of duties allow for balance between control and innovation. Central operations can maintain centralized operations for workloads that require increase compliance, stable state operations, or represent greater security risks. Conversely, this approach allows for reduction in centralized control of workloads and environments that require greater innovation. Since larger portfolios are more likely to struggle with the balance between control and innovation, this flexibility makes it easier to scale to thousands of workloads with reductions in operational pains.
- **Distinct disadvantage:** What worked well on-premises might not work well in enterprise cloud operations. This approach to operations requires changes on many fronts. Cultural shifts in control and responsibility are often the biggest challenge. Operational shifts that follow the cultural shift take time and committed effort to implement, mature, and stabilize. Architectural shifts are sometimes required in otherwise stable workloads. Tooling shifts are required to empower and support the cultural, operational, and architectural shifts, which might require commitments to a primary cloud provider. Adoption efforts made prior to these changes might

require significant rework that goes beyond typical refactoring efforts.

- **Risk:** This approach requires executive commitment to the change strategy. It also requires commitment from the technical teams to overcome learning curves and deliver the required change. Long-term cooperation between business, CCoE/central IT, and workload teams is required to see long-term benefits.
- **Guidance:** Azure landing zone implementation options defined as "enterprise-scale" provide reference implementations to demonstrate how the technical changes are delivered using cloud-native tooling in Azure. The enterprise-scale approach guides teams through the operational and cultural shifts required to take full advantage of those implementations. That same approach can be used to tailor the reference architecture to configure the environment to meet your adoption strategy and compliance constraints. Once enterprise-scale has been implemented, the Govern and Manage methodologies can be used to define processes and expand your compliance and operations capabilities to meet your specific operational needs.

### **Advantages of enterprise operations**

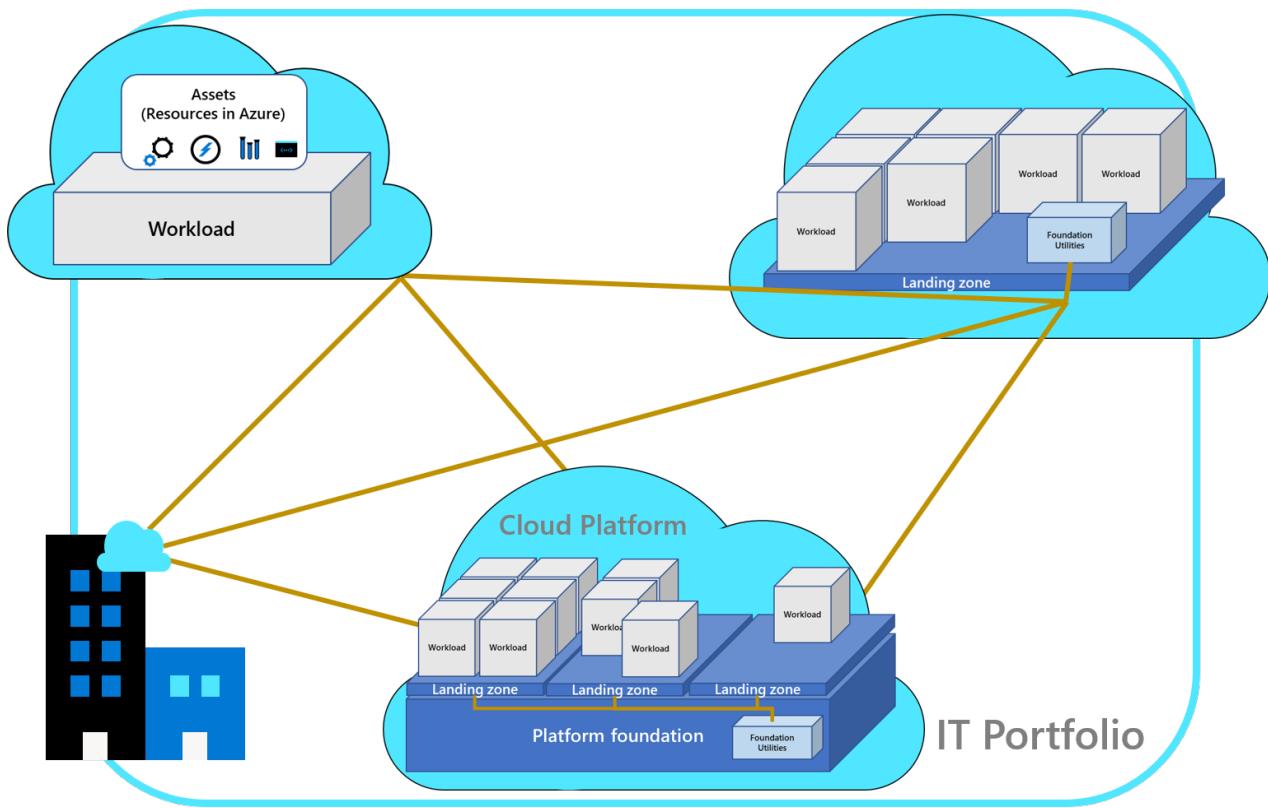
- **Cost management:** Central teams act on cross-portfolio optimizations and hold individual workload teams accountable for deeper workload optimization. Workload focused teams are empowered to make decisions and provided clarity when those decisions have a negative cost impact. Central and workload teams share accountability for cost decisions at the right level.
- **Responsibilities:** Central teams use cloud-native tools to define, enforce, and automate guardrails. Efforts of the workload teams are accelerated through CCoE automation and practices. The workload teams are then empowered to drive innovation and make decisions within those guardrails.
- **Standardization:** Centralized guardrails and foundational services create consistency across all environments, regardless of scale.
- **Operations support:** Workloads that require centralized operations support are segmented to environments with stable-state controls. Segmentation and separation of duties empower workload teams to take accountability for operational support in their own dedicated environments. Automated, cloud native tools ensure a minimum operations baseline for all environments with centralized operational support for the baseline offering.
- **Expertise:** Centralization of core services such as security, risk, governance, and operations ensures proper central expertise. Clear processes and guardrails educates and empowers all members of the workload teams to make more detailed decisions that expand the impact of the centralized experts, without needing to scale that staff linearly with technology scale.
- **Landing zone design:** Landing zone design replicates the needs of the portfolio, creating clear security, governance, and accountability boundaries required to operate workloads in the cloud. Segmentation practices are unlikely to resemble the constraints created by preceding datacenter designs. In enterprise operations, landing-zone design is less complex, allowing for faster scale and reduced barriers to self-service demand.
- **Foundational utilities:** Foundational utilities are hosted in separate centrally controlled subscriptions referred to as the platform foundation. Central tools are then "piped" into each landing zone as a utility services. Separating foundational utilities from the landing zones maximizes consistency, economy of scale, and creates clear distinctions between centrally managed responsibilities and workload level responsibilities.
- **Separation of duties:** Clear separation of duties between foundational utilities and landing zones is one of the biggest advantages of this approach to operations. Cloud-native tools and sound processes allow for just-in-time access and proper balance of control between centralized teams and workload teams, based on the requirements of the individual landing zones and the workloads hosted in those landing zone segments.

### **Disadvantages of enterprise operations**

- **Cost management:** Central teams are more dependent on workload teams to make production changes within landing zones. This shift does create a risk of potential budget overruns and slower right-sizing of actual spend. Cost control processes, clear budgets, automated controls, and regular reviews must be in place early to avoid cost surprises.
- **Responsibilities:** Enterprise operations requires greater cultural and operational requirements on central and workload teams to ensure clarity in responsibilities and accountability between teams.

- Traditional change management processes or change advisory boards (cabs) are less likely to maintain the pace and balance required in this operating model. Those processes should be reflected in the automation of processes and procedures to safely scale cloud adoption.
- Lack of commitment to change will first materialize in negotiation and alignment of responsibilities. Inability to align on shifts in responsibility is an indication that central IT operating models might be required during short-term cloud adoption efforts.
- **Standardization:** Lack of investment in centralized guardrails or automation create risks to standardization that are more difficult to overcome through manual review processes. Additionally, operational dependencies between workloads in the landing zones and shared services in the platform foundation creates greater risk to standardization during upgrade cycles or future versions of the foundational utilities. During platform foundation revisions, improved or even automated testing is required of all supported landing zones and the workloads they host.
- **Operations support:** The operations baseline provided through automation and centralized operations might be sufficient for low impact or low criticality workloads. However, workload teams or other forms of dedicated operations will likely be required for complex or high criticality workloads. This might necessitate a shift in operations budgets, requiring business units to allocate operating expenses to those forms of advanced operations. If central IT is required to maintain sole accountability for the cost of operations, then enterprise operations will be difficult to implement.
- **Expertise:** Central IT team members will be required to develop expertise regarding automation of central controls previously delivered via manual processes. Those teams might also need to develop a proficiency for infrastructure-as-code approaches to defining the environment, along with an understanding of branching, merging, and deployment pipelines. At a minimum, a platform automation team will need these skills to act on decisions made by the cloud center of excellence or central operations teams. Workload teams will be required to develop additional knowledge related to the controls and processes that will govern their decisions.
- **Landing zone design:** Landing zone design takes a dependency on the foundational utilities. To avoid duplication of effort (or errors/conflicts with automated governance), each workload focused team should understand what is included in the design and what is forbidden. Exception processes should also be factored in to landing zone designs to create flexibility.
- **Foundational utilities:** Centralization of foundational utilities does take some time to consider options and develop a solution that will scale to meet various adoption plans. This can delay early adoption efforts, but should be offset in the long term by accelerations and blocker avoidance later in the process.
- **Separation of duties:** Ensuring clear separation of duties does require mature identity management processes. There might be additional maintenance associated with the proper alignment of users, groups, and onboarding/off-boarding activities. New processes will likely be needed to accommodate just-in-time access via elevated privileges.

## Distributed operations



The existing operating model might be too engrained for the entire organization to shift to a new operating model. For others, global operations and various compliance requirements might prevent specific business units from making a change. For those companies, a distributing operations approach might be required. This is by far the most complex approach, as it requires an integration of one or more of the previously mentioned operating models.

While heavily discouraged, this approach to operations might be required for some organizations who consist of a loose collection of disparate business units. Especially when those business units span a diverse base of customer segments or regional operations.

- **Priorities:** Integration of multiple existing operating models.
- Transitional state with a focus on moving the entire organization to one of the previously mentioned operating models, over time.
- Longer term operational approach when the organization is too large or too complex to align to a single operating model.
- **Distinct advantage:** Integration of common operating model elements from each business unit. Creates a vehicle to group operating units into a hierarchy and help them mature operations using consistent repeatable processes.
- **Distinct disadvantage:** Consistency and standardization across multiple operating models is difficult to maintain for extended periods. This operational approach requires deep awareness of the portfolio and how various segments of the technology portfolio are operated.
- **Risk:** Lack of commitment to a primary operating model could lead to confusion across teams. This operating model should only be used when there is no way to align to a single operating model.
- **Guidance:** Start with a thorough review of the portfolio using the approach outlined in the [business alignment](#) articles. Take care to group the portfolio by desired state operating model (decentralized, centralized, or enterprise).
- Develop a management group hierarchy that reflects the operating model groupings, followed by other organizational patterns for region, business unit, or other criteria that map the workload clusters from least common to most common buckets.
- Evaluate the alignment of workloads to operating models to find the most relevant operating model cluster to start with. Follow the guidance that maps to that operating model for all workloads under that node of the

management group hierarchy.

- Use the Govern and Manage methodologies to find common corporate policies and required operational management practices at various points of the hierarchy. Apply common Azure policies to automate the shared corporate policies.
- As those Azure policies are tested with various deployments, attempt to move them higher in the management group hierarchy applying those policies to greater numbers of workloads to find commonalities and distinct operation needs.
- Over time this approach will help define an operating model that scales across your various other operating models and unifies teams through a set of common policies and procedures.

Advantages and disadvantages of this approach are purposefully blank. After you complete the business alignment of your portfolio, see the predominant operating model section above for clarity on advantages and disadvantages.

## Next steps

Learn the terminology associated with operating models. The terminology helps you understand how an operating model fits into the bigger theme of corporate planning.

[Operating model terminology](#)

Learn how a landing zone provides the basic building block of any cloud adoption environment.

[Compare common cloud operating models](#)

# Operating model terminology

11/9/2020 • 2 minutes to read • [Edit Online](#)

The term operating model has many definitions. This intro article establishes terminology associated with operating models. To understand an operating model as it relates to the cloud, we first have to understand how an operating model fits into the bigger theme of corporate planning.

## Terms

**Business model:** Business models tend to define corporate value (*what* the business does to provide value) and mission/vision statements (*why* the business has chosen to add value in that way). At a minimum, business models should be able to represent the *what* and *why* in the form of financial projections. There are many different schools of thought regarding how far a business model goes beyond these basic leadership principles. However, to create a sound operating model, the business models should include high-level statements to establish directional goals. It's even more effective if those goals can be represented in metrics or KPIs to track progress.

**Customer experience:** All good business models ground the *why* side of a business's strategy in the experience of their customers. This process could involve a customer acquiring a product or service. It could include interactions between a company and its business customers. Another example could center around the long-term management of a customer's financial or health needs, as opposed to a single transaction or process. Regardless of the type of experience, the majority of successful companies realize that they exist to operate and improve the experiences that drive their *why* statements.

**Digital transformation:** Digital transformation has become an industry buzzword. However, it is a vital component in the fulfillment of modern business models. Since the advent of the smartphone and other portable computing form factors, customer experiences have become increasingly digital. This shift is painfully obvious in some industries like DVD rentals, print media, automotive, or retail. In each case, digitized experiences have had a significant impact on the customer experience. In some cases, physical media have been entirely replaced with digital media, upsetting the entire industry vertical. In others, digital experiences are seen as a standard augmentation of the experience. To deliver business value (*what* statements), the customer experience (*why* statements) must factor in the impact of digital experiences on the customers' experiences. This process is digital transformation. Digital transformation is seldom the entire *why* statement in a business strategy, but it is an important aspect.

**Operating model:** If the business model represents the *what* and *why*, then an operating model represents the *how* and *who* for operationalizing the business strategy. The operating model defines the ways in which people work together to accomplish the large goals outlined in the business strategy. Operating models are often described as the people, process, and technology behind the business strategy. In the article on the Cloud Adoption Framework operating model, this concept is explained in detail.

**Cloud adoption:** As stated above, digital transformation is an important aspect of the customer experience and the business model. Likewise, cloud adoption is an important aspect of any operating model. Cloud adoption is a strong enabler to deliver the right technologies and processes required to successfully deliver on the modern operating model.

Cloud adoption is *what we do* to realize the business value. The operating model represents *who we are* and how we function on a daily basis while cloud adoption is being delivered.

## Take action

[Use the operating model](#) provided by the Cloud Adoption Framework to develop operational maturity.

## Next steps

Continue to the next section of the Cloud Adoption Framework. Learn how a landing zone provides the basic building block of any cloud adoption environment.

[Use the operating model](#)

# What is an Azure landing zone?

11/9/2020 • 2 minutes to read • [Edit Online](#)

Azure landing zones are the output of a multisubscription Azure environment that accounts for scale, security, governance, networking, and identity. Azure landing zones enable application migrations and greenfield development at an enterprise scale in Azure. These zones consider all platform resources that are required to support the customer's application portfolio and don't differentiate between infrastructure as a service or platform as a service.

## Scalable and modular

No single solution fits all technical environments. A few Azure landing zone implementation options can help you meet the deployment and operations needs of your growing cloud portfolio. All Azure landing zones provide a scalable, modular approach to building out your environment based on a common set of design areas. Whether you're looking to deploy your first production application to Azure or you're operating a complex portfolio of workloads, the Azure landing zone implementation options can be tailored to your needs.

## Next steps

When you're choosing the right Azure landing zone implementation option, you should understand the [Azure landing zone design areas](#).

[Review design areas](#)

# Design areas of a well-architected landing zone

11/9/2020 • 2 minutes to read • [Edit Online](#)

Each Azure landing zone implementation option provides a deployment approach and defined design principles. Before choosing an implementation option, use this article to gain an understanding of the design areas listed in the following table.

## NOTE

These design areas describe what you should consider prior to deploying a landing zone. Use it as a simple reference. See the [landing zone implementation options](#) for design principles and actionable steps for deployment.

## Design areas

Regardless of the deployment option, you should carefully consider each design area. Your decisions affect the platform foundation on which each landing zone depends.

DESIGN AREAS	OBJECTIVE	RELEVANT METHODOLOGIES
Enterprise enrollment	For enterprise customers with an Azure commitment, proper tenant creation and enrollment is an important early step.	Ready
Identity	Identity and access management is a primary security boundary in the public cloud. It's the foundation for any secure and fully compliant architecture.	Ready
Network topology and connectivity	Networking and connectivity decisions are an equally important foundational aspect of any cloud architecture.	Ready
Resource organization	As cloud adoption scales, considerations for subscription design and management group hierarchy have an impact on governance, operations management, and adoption patterns.	Govern
Governance disciplines	Automate auditing and enforcement of security, governance, and compliance policies.	Govern
Operations baseline	For stable, ongoing operations in the cloud, an operations baseline is required to provide visibility, operations compliance, and protect and recover capabilities.	Manage

DESIGN AREAS	OBJECTIVE	RELEVANT METHODOLOGIES
Business continuity and disaster recovery (BCDR)	Resiliency is key for smooth functioning of applications. BCDR is an important component of resiliency. BCDR involves protection of data via backups and protection of applications from outages via disaster recovery.	Manage
Deployment options	Align the best tools and templates to deploy your landing zones and supporting resources.	Ready

## Next steps

You can implement these design areas over time so that you can grow into your cloud operating model. Alternately, there are rich, opinionated implementation options that start with a defined position on each design area.

With an understanding of the modular design areas, the next step is to choose the [landing zone implementation option](#) that best aligns with your cloud adoption plan and requirements.

[Choose an implementation option](#)

# Landing zone implementation options

11/9/2020 • 3 minutes to read • [Edit Online](#)

Azure landing zones provide cloud adoption teams with a well-managed environment for their workloads.

Follow the [landing zone design areas](#) guidance to take advantage of these capabilities.

Each of the following implementation options is designed for a specific set of operating model dependencies to support your nonfunctional requirements. Each implementation option includes distinct automation approaches. When available, reference architectures and reference implementations are included to accelerate your cloud adoption journey. While each option is mapped to a different operating model, they share the same design areas. The difference is how you choose to implement them.

## Platform development velocity

In addition to the recommended design areas, your platform development velocity (how fast your platform team can develop the required skills) is a key factor when choosing the best deployment option. Consider two primary modes:

**Start with enterprise scale:** Use this mode if your business requirements necessitate a rich initial implementation of landing zones with fully integrated governance, security, and operations from the start. With this approach, you can use either the Azure portal or infrastructure-as-code to set up and configure your environment. You can also transition between the portal and infrastructure-as-code (recommended) when your organization is ready. Infrastructure-as-code approaches require skills in Azure Resource Manager templates and GitHub.

**Start small and expand:** Use this mode if it's more important to develop these skills and commit to your decisions as you learn more about the cloud. In this approach, the landing zones only focus on implementing the basic landing zones considerations required to start cloud adoption. As your adoption expands, modules in the Govern and Manage methodologies will build on top of your initial landing zones. The design principles of any Azure landing zone outline the specific design areas that will require refactoring over time.

## Implementation options

The following table describes some of the implementation options for landing zones and the variables that might drive your decision.

IMPLEMENTATION OPTION	DESCRIPTION	DEPLOYMENT VELOCITY	DEEPER DESIGN PRINCIPLES	DEPLOYMENT INSTRUCTIONS
CAF Migration landing zone blueprint	Deploys the basic foundation for migrating low risk assets.	Start small	<a href="#">Design principles</a>	Deploy
CAF Foundation blueprint	Adds the minimum tools need to begin developing a governance strategy.	Start small	<a href="#">Design principles</a>	Deploy

IMPLEMENTATION OPTION	DESCRIPTION	DEPLOYMENT VELOCITY	DEEPER DESIGN PRINCIPLES	DEPLOYMENT INSTRUCTIONS
CAF enterprise-scale landing zone (hybrid connectivity with vWan)	Deploys an enterprise-ready platform foundation with all the necessary shared services to support the full IT portfolio, including hybrid connectivity (vWAN).	Enterprise-scale	Design principles	Deploy
CAF enterprise-scale landing zone (hybrid connectivity with hub & spoke)	Deploys an enterprise-ready platform foundation with all the necessary shared services to support the full IT portfolio, including hybrid connectivity (Hub & Spoke).	Enterprise-scale	Design principles	Deploy
CAF enterprise-scale landing zone	Deploys an enterprise-ready platform foundation with all the necessary shared services to support the full IT portfolio, where connectivity can be added later as needed.	Enterprise-scale	Design principles	Deploy
CAF Terraform modules	Third-party path for multicloud operating models. This path can limit Azure-first operating models.	Start small	Design principles	Deploy
Partner landing zones	Partners who provide offerings aligned to the Ready methodology of the Cloud Adoption Framework can provide their own customized implementation option.	Variable	Design principles	Find a partner

The following table looks at some of these implementation options from a slightly different perspective to guide more technical decision processes.

IMPLEMENTATION OPTION	HUB	SPOKE	DEPLOYMENT TECHNOLOGY	DEPLOYMENT INSTRUCTIONS
Cloud Adoption Framework enterprise-scale landing zone	Included	Included	Azure Resource Manager templates, Azure portal, Azure Policy and GitHub	<a href="#">Deploy</a>
Cloud Adoption Framework migration landing zone blueprint	Refactor required	Included	Azure Resource Manager templates, Azure portal, and Azure Blueprints	<a href="#">Deploy</a>
Cloud Adoption Framework Terraform modules	Included in virtual datacenter module	Included	Terraform	<a href="#">Deploy</a>

## Next steps

To proceed, choose one of the implementation options shown in the preceding table. Each option includes a link to deployment instructions and the specific design principles that guide implementation.

# Start with Cloud Adoption Framework enterprise-scale landing zones

11/9/2020 • 2 minutes to read • [Edit Online](#)

The enterprise-scale architecture represents the strategic design path and target technical state for your Azure environment. It will continue to evolve alongside the Azure platform and is defined by the various design decisions that your organization must make to map your Azure journey.

Not all enterprises adopt Azure in the same way, so the Cloud Adoption Framework for Azure enterprise-scale landing zone architecture varies between customers. The technical considerations and design recommendations of the enterprise-scale architecture might lead to different trade-offs based on your organization's scenario. Some variation is expected, but if you follow the core recommendations, the resulting target architecture will set your organization on a path to sustainable scale.

## Prescriptive guidance

The enterprise-scale architecture provides prescriptive guidance coupled with Azure best practices. It follows design principles across the critical design areas for an organization's Azure environment.

## Qualifiers: Should I start with enterprise scale?

The enterprise-scale architecture is modular by design. It allows you to start with foundational landing zones that support your application portfolios, no matter whether the applications are being migrated or are newly developed and deployed to Azure. The architecture can scale alongside your business requirements regardless of scale point.

## Start with a Cloud Adoption Framework enterprise-scale landing zone

The enterprise-scale approach to construct landing zones includes three sets of assets to support cloud teams:

- [Design guidelines](#): Guide to the critical decisions that drive the design of the Cloud Adoption Framework for Azure enterprise-scale landing zone.
- [Architecture](#): Conceptual reference architecture that demonstrates design areas and best practices.
- [Implementations](#): Azure Resource Manager template of the architecture to accelerate adoption.

## Community

This guide is developed largely by Microsoft architects and the broader Cloud Solutions Unit technical community. This community actively advances this guide to share lessons learned during enterprise-scale adoption efforts.

This guide shares the same design principles as the standard Ready methodology. It expands on those principles to integrate subjects such as governance and security earlier in the planning process. Expanding the standard process is necessary because of a few natural assumptions that can be made when an adoption effort requires large-scale enterprise change.

## Next steps

[Implement a Cloud Adoption Framework enterprise-scale landing zone](#)

# Implement Cloud Adoption Framework enterprise-scale landing zones in Azure

11/9/2020 • 2 minutes to read • [Edit Online](#)

When business requirements necessitate a rich initial implementation of landing zones with fully integrated governance, security, and operations from the start, use the enterprise-scale example options listed here. With this approach, you can use the Azure portal or infrastructure as code to set up and configure your environment. It's also possible to transition between the portal and infrastructure as code (recommended) when your organization is ready.

## Example implementation

The following table lists example modular implementations.

EXAMPLE DEPLOYMENT	DESCRIPTION	GITHUB REPO	DEPLOY TO AZURE
Enterprise-scale foundation	This is the suggested foundation for enterprise-scale adoption.	<a href="#">Example in GitHub</a>	<a href="#">Deploy example to Azure</a>
Enterprise-scale Virtual WAN	Add a Virtual WAN network module to the enterprise-scale foundation.	<a href="#">Example in GitHub</a>	<a href="#">Deploy example to Azure</a>
Enterprise-scale hub and spoke	Add a hub-and-spoke network module to the enterprise-scale foundation.	<a href="#">Example in GitHub</a>	<a href="#">Deploy example to Azure</a>

## Next steps

These examples provide an easy deployment option to support continued learning for the enterprise-scale approach. Before you use these examples in a production version of enterprise scale, review the [enterprise-scale architecture](#).

# Cloud Adoption Framework enterprise-scale landing zone architecture

11/9/2020 • 4 minutes to read • [Edit Online](#)

Enterprise-scale is an architectural approach and a reference implementation that enables effective construction and operationalization of landing zones on Azure, at scale. This approach aligns with the Azure roadmap and the Cloud Adoption Framework for Azure.

## Architecture overview

The Cloud Adoption Framework enterprise-scale landing zone architecture represents the strategic design path and target technical state for an organization's Azure environment. It will continue to evolve alongside the Azure platform and is defined by the various design decisions that your organization must make to map your Azure journey.

Not all enterprises adopt Azure the same way, so the Cloud Adoption Framework enterprise-scale landing zone architecture varies between customers. The technical considerations and design recommendations in this guide might yield different trade-offs based on your organization's scenario. Some variation is expected, but if you follow the core recommendations, the resulting target architecture will set your organization on a path to sustainable scale.

## Landing Zone in enterprise-scale

Azure landing zones are the output of a multisubscription Azure environment that accounts for scale, security, governance, networking, and identity. Azure landing zones enable application migrations and greenfield development at an enterprise scale in Azure. These zones consider all platform resources that are required to support the customer's application portfolio and don't differentiate between infrastructure as a service or platform as a service.

An example is how city utilities such as water, gas, and electricity are accessible before new homes are constructed. In this context, the network, identity and access management, policies, management, and monitoring are shared utility services that must be readily available to help streamline the application migration process before it begins.

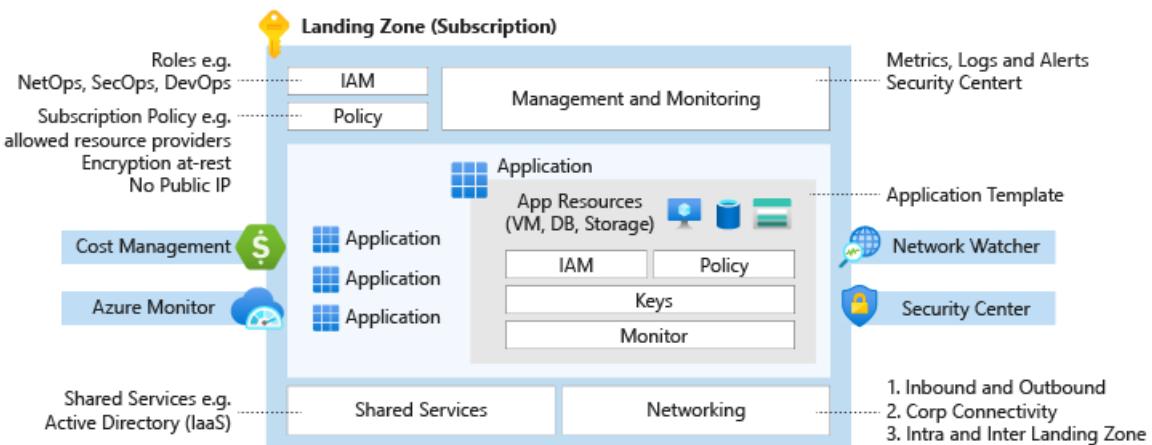


Figure 1: Landing zone design.

## High-level architecture

An Enterprise-Scale architecture is defined by a set of design considerations and recommendations across eight

[critical design areas](#), with two network topologies recommended: an Enterprise-Scale architecture based on an Azure Virtual WAN network topology (depicted on figure 2), or based on a traditional Azure network topology based on the hub and spoke architecture (depicted on figure 3).

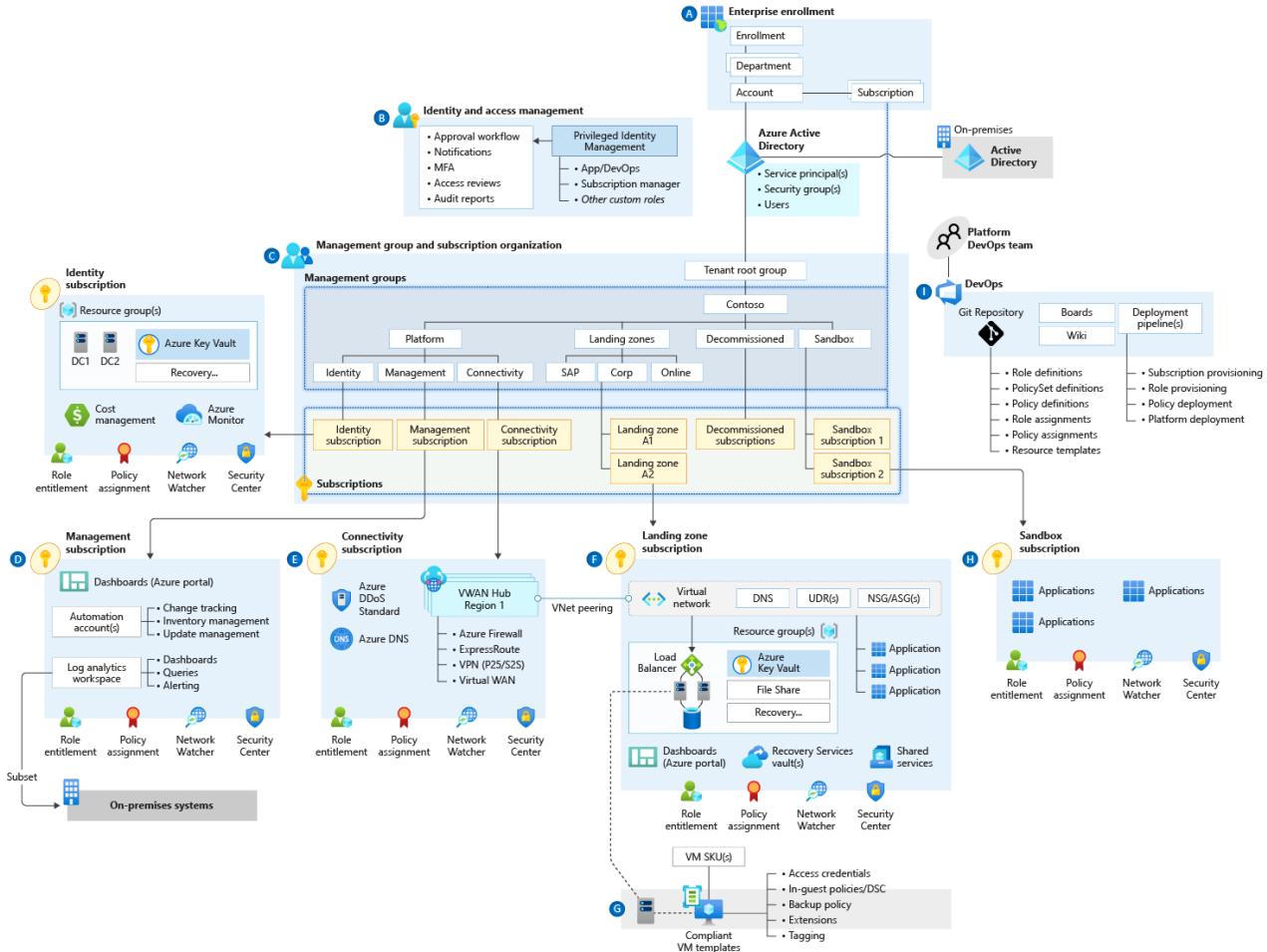


Figure 2: Cloud Adoption Framework enterprise-scale landing zone architecture based on an Azure Virtual WAN network topology.

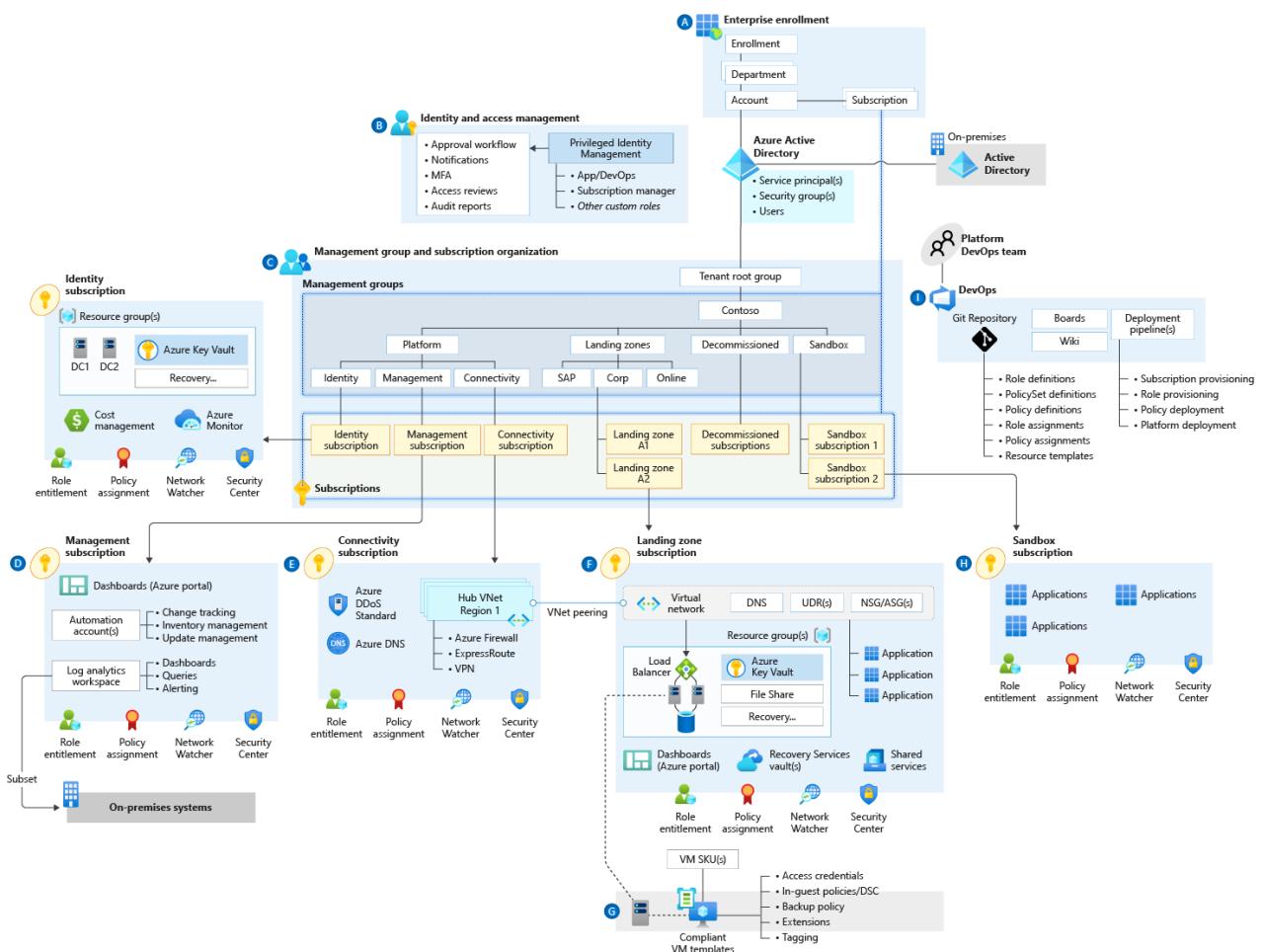


Figure 3: Cloud Adoption Framework enterprise-scale landing zone architecture based on a traditional Azure networking topology.

Download the PDF files that contain the Enterprise-Scale architecture diagrams based on the [Virtual WAN](#) network topology or a traditional Azure network topology based on the [hub and spoke](#) architecture.

On figures 2 and 3 there are references to the Enterprise-Scale critical design areas, which are indicated with the letters A to I:

**A Enterprise Agreement (EA) enrollment and Azure Active Directory tenants.** An Enterprise Agreement (EA) enrollment represents the commercial relationship between Microsoft and how your organization uses Azure. It provides the basis for billing across all your subscriptions and affects administration of your digital estate. Your EA enrollment is managed via an Azure enterprise portal. An enrollment often represents an organization's hierarchy, which includes departments, accounts, and subscriptions. An Azure AD tenant provides identity and access management, which is an important part of your security posture. An Azure AD tenant ensures that authenticated and authorized users have access to only the resources for which they have access permissions.

**B Identity and access management.** Azure Active Directory design and integration must be built to ensure both server and user authentication. Resource-based access control (RBAC) must be modeled and deployed to enforce separation of duties and the required entitlements for platform operation and management. Key management must be designed and deployed to ensure secure access to resources and support operations such as rotation and recovery. Ultimately, access roles are assigned to application owners at the control and data planes to create and manage resources autonomously.

**C Management group and subscription organization.** Management group structures within an Azure Active Directory (Azure AD) tenant support organizational mapping and must be considered thoroughly when an organization plans Azure adoption at scale. Subscriptions are a unit of management, billing, and scale within Azure. They play a critical role when you're designing for large-scale Azure adoption. This critical design area helps you capture subscription requirements and design target subscriptions based on critical factors. These factors are

environment type, ownership and governance model, organizational structure, and application portfolios.

**D Management and monitoring.** Platform-level holistic (horizontal) resource monitoring and alerting must be designed, deployed, and integrated. Operational tasks such as patching and backup must also be defined and streamlined. Security operations, monitoring, and logging must be designed and integrated with both resources on Azure and existing on-premises systems. All subscription activity logs that capture control plane operations across resources should be streamed into Log Analytics to make them available for query and analysis, subject to RBAC permissions.

**E Network topology and connectivity.** The end-to-end network topology must be built and deployed across Azure regions and on-premises environments to ensure north-south and east-west connectivity between platform deployments. Required services and resources such as firewalls and network virtual appliances must be identified, deployed, and configured throughout network security design to ensure that security requirements are fully met.

**F, G, H Business continuity and disaster recovery** and **Security, governance, and compliance.** Holistic and landing-zone-specific policies must be identified, described, built, and deployed onto the target Azure platform to ensure corporate, regulatory, and line-of-business controls are in place. Ultimately, policies should be used to guarantee the compliance of applications and underlying resources without any abstraction provisioning or administration capability.

**I Platform automation and DevOps.** An end-to-end DevOps experience with robust software development lifecycle practices must be designed, built, and deployed to ensure a safe, repeatable, and consistent delivery of infrastructure-as-code artifacts. Such artifacts are to be developed, tested, and deployed by using dedicated integration, release, and deployment pipelines with strong source control and traceability.

## Next steps

Customize implementation of this architecture by using the Cloud Adoption Framework enterprise-scale design guidelines.

[Design guidelines](#)

# Cloud Adoption Framework enterprise-scale design principles

11/9/2020 • 2 minutes to read • [Edit Online](#)

The enterprise-scale architecture prescribed in this guidance is based on the design principles described here. These principles serve as a compass for subsequent design decisions across critical technical domains. Familiarize yourself with these principles to better understand their impact and the trade-offs associated with nonadherence.

## Subscription democratization

Subscriptions should be used as a unit of management and scale aligned with business needs and priorities to support business areas and portfolio owners to accelerate application migrations and new application development. Subscriptions should be provided to business units to support the design, development, and testing of new workloads and migration of workloads.

## Policy-driven governance

Azure Policy should be used to provide guardrails and ensure continued compliance with your organization's platform, along with the applications deployed onto it. Azure Policy also provides application owners with sufficient freedom and a secure unhindered path to the cloud.

## Single control and management plane

Enterprise-scale architecture shouldn't consider any abstraction layers, such as customer-developed portals or tooling. It should provide a consistent experience for both AppOps (centrally managed operation teams) and DevOps (dedicated application operation teams). Azure provides a unified and consistent control plane across all Azure resources and provisioning channels subject to role-based access and policy-driven controls. Azure can be used to establish a standardized set of policies and controls for governing the entire enterprise estate.

## Application-centric and archetype-neutral

Enterprise-scale architecture should focus on application-centric migrations and development rather than pure infrastructure lift-and-shift migrations, such as moving virtual machines. It shouldn't differentiate between old and new applications, infrastructure as a service, or platform as a service applications. Ultimately, it should provide a safe and secure foundation for all application types to be deployed onto your Azure platform.

## Align Azure-native design and roadmaps

The enterprise-scale architecture approach advocates using Azure-native platform services and capabilities whenever possible. This approach should align with Azure platform roadmaps to ensure that new capabilities are available within your environments. Azure platform roadmaps should help to inform the migration strategy and enterprise-scale trajectory.

## Recommendations

Be prepared to trade off functionality because it's unlikely that everything will be required on day one. Use preview services and take dependencies on service roadmaps to remove technical blockers.

# Cloud Adoption Framework enterprise-scale design guidelines

11/9/2020 • 2 minutes to read • [Edit Online](#)

This article and the articles series that follows outline how the enterprise-scale architecture provides an opinionated position on each of the [Azure landing zone design areas](#). This series provides a step-by-step set of design guidelines that can be followed to implement the design principles embodied in the enterprise-scale solution.

The core of enterprise-scale architecture contains a critical design path comprised of fundamental design topics with heavily interrelated and dependent design decisions. This repo provides design guidance across these architecturally significant technical domains to support the critical design decisions that must occur to define the enterprise-scale architecture. For each of the considered domains, review the provided considerations and recommendations and use them to structure and drive designs within each area.

For example, you might ask how many subscriptions are needed for your estate. You can review [subscription organization and governance](#) and use the outlined recommendations to drive subscription decisions.

## Critical design areas

The following eight critical design areas can help you translate your requirements to Azure constructs and capabilities. These design areas can help you address the mismatch between on-premises and cloud-design infrastructure, which typically creates dissonance and friction between the enterprise-scale definition and Azure adoption.

The impact of decisions made within these critical areas will reverberate across enterprise-scale architecture and influence other decisions. Familiarize yourself with these eight areas to better understand the consequences of encompassed decisions, which could later produce trade-offs within related areas.

- [Enterprise Agreement \(EA\) enrollment and Azure Active Directory tenants](#)
- [Identity and access management](#)
- [Management group and subscription organization](#)
- [Network topology and connectivity](#)
- [Management and monitoring](#)
- [Business continuity and disaster recovery](#)
- [Security, governance, and compliance](#)
- [Platform automation and DevOps](#)

# Enterprise Agreement enrollment and Azure Active Directory tenants

11/9/2020 • 3 minutes to read • [Edit Online](#)

## Plan for enterprise enrollment

An Enterprise Agreement (EA) enrollment represents the commercial relationship between Microsoft and how your organization uses Azure. It provides the basis for billing across all your subscriptions and affects administration of your digital estate. Your EA enrollment is managed via an Azure enterprise portal. An enrollment often represents an organization's hierarchy, which includes departments, accounts, and subscriptions. This hierarchy represents cost-enrollment groups within an organization.

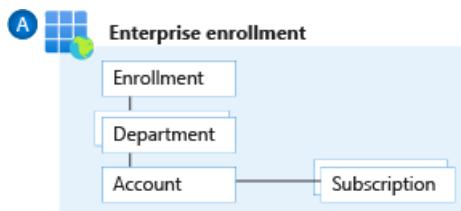


Figure 1: An Azure EA enrollment hierarchy.

- Departments help to segment costs into logical groupings and to set a budget or quota at the department level. The quota isn't enforced firmly and is used for reporting purposes.
- Accounts are organizational units in the Azure enterprise portal. They can be used to manage subscriptions and access reports.
- Subscriptions are the smallest unit in the Azure enterprise portal. They're containers for Azure services managed by the service administrator. They're where your organization deploys Azure services.
- EA enrollment roles link users with their functional role. These roles are:
  - Enterprise administrator
  - Department administrator
  - Account owner
  - Service administrator
  - Notification contact

### Design considerations:

- The enrollment provides a hierarchical organizational structure to govern the management of subscriptions.
- Multiple environments can be separated at an EA-account level to support holistic isolation.
- There can be multiple administrators appointed to a single enrollment.
- Each subscription must have an associated account owner.
- Each account owner will be made a subscription owner for any subscriptions provisioned under that account.
- A subscription can belong to only one account at any given time.
- A subscription can be suspended based on a specified set of criteria.

### Design recommendations:

- Only use the authentication type `Work or school account` for all account types. Avoid using the `Microsoft account (MSA)` account type.
- Set up the notification contact email address to ensure notifications are sent to an appropriate group mailbox.

- Assign a budget for each account, and establish an alert associated with the budget.
- An organization can have a variety of structures, such as functional, divisional, geographic, matrix, or team structure. Use organizational structure to map your organization structure to your enrollment hierarchy.
- Create a new department for IT if business domains have independent IT capabilities.
- Restrict and minimize the number of account owners within the enrollment to avoid the proliferation of admin access to subscriptions and associated Azure resources.
- If multiple Azure Active Directory (Azure AD) tenants are used, verify that the account owner is associated with the same tenant as where subscriptions for the account are provisioned.
- Set up Enterprise Dev/Test and production environments at an EA account level to support holistic isolation.
- Don't ignore notification emails sent to the notification account email address. Microsoft sends important EA-wide communications to this account.
- Don't move or rename an EA account in Azure AD.
- Periodically audit the EA portal to review who has access and avoid using a Microsoft account where possible.

## Define Azure AD tenants

An Azure AD tenant provides identity and access management, which is an important part of your security posture. An Azure AD tenant ensures that authenticated and authorized users have access to only the resources for which they have access permissions. Azure AD provides these services to applications and services deployed in Azure and also to services and applications deployed outside of Azure (such as on-premises or third-party cloud providers).

Azure AD is also used by software as a service applications such as Microsoft 365 and Azure Marketplace. Organizations already using on-premises Active Directory can use their existing infrastructure and extend authentication to the cloud by integrating with Azure AD. Each Azure AD directory has one or more domains. A directory can have many subscriptions associated with it but only one Azure AD tenant.

Ask basic security questions during the Azure AD design phase, such as how your organization manages credentials and how it controls human, application, and programmatic access.

### Design considerations:

- Multiple Azure AD tenants can function in the same enrollment.

### Design recommendations:

- Use Azure AD seamless single sign-on based on the selected [planning topology](#).
- If your organization doesn't have an identity infrastructure, start by implementing an Azure-AD-only identity deployment. Such deployment with [Azure AD Domain Services](#) and [Microsoft Enterprise Mobility + Security](#) provides end-to-end protection for SaaS applications, enterprise applications, and devices.
- Multifactor authentication provides another layer of security and a second barrier of authentication. Enforce [multifactor authentication](#) and [conditional access policies](#) for all privileged accounts for greater security.
- Plan and implement for [emergency access](#) or break-glass accounts to prevent tenant-wide account lockout.
- Use [Azure AD Privileged Identity Management](#) for identity and access management.
- If dev/test and production are going to be isolated environments from an identity perspective, separate them at a tenant level via multiple tenants.
- Avoid creating a new Azure AD tenant unless there's a strong identity and access management justification and processes are already in place.

# Identity and access management

11/9/2020 • 6 minutes to read • [Edit Online](#)

Identity provides the basis of a large percentage of security assurance. It enables access based on identity authentication and authorization controls in cloud services to protect data and resources and to decide which requests should be permitted.

Identity and access management (IAM) is boundary security in the public cloud. It must be treated as the foundation of any secure and fully compliant public cloud architecture. Azure offers a comprehensive set of services, tools, and reference architectures to enable organizations to make highly secure, operationally efficient environments as outlined here.

This section examines design considerations and recommendations related to IAM in an enterprise environment.

## Why we need identity and access management

The technological landscape in the enterprise is becoming complex and heterogeneous. To manage compliance and security for this environment, IAM enables the right individuals to access the right resources at the right time for the right reasons.

### Plan for identity and access management

Enterprise organizations typically follow a least-privileged approach to operational access. This model should be expanded to consider Azure through Azure Active Directory (Azure AD) role-based access control (RBAC) and custom role definitions. It's critical to plan how to govern control- and data-plane access to resources in Azure. Any design for IAM and RBAC must meet regulatory, security, and operational requirements before it can be accepted.

Identity and access management is a multistep process that involves careful planning for identity integration and other security considerations, such as blocking legacy authentication and planning for modern passwords. Staging planning also involves selection of business-to-business or business-to-consumer identity and access management. While these requirements vary, there are common design considerations and recommendations to consider for an enterprise landing zone.



Figure 1: Identity and access management.

### Design considerations:

- There are limits around the number of custom roles and role assignments that must be considered when you lay down a framework around IAM and governance. For more information, see [Azure RBAC service limits](#).
- There's a limit of 2,000 custom RBAC role assignments per subscription.
- There's a limit of 500 custom RBAC role assignments per management group.
- Centralized versus federated resource ownership:
  - Shared resources or any aspect of the environment that implements or enforces a security boundary, such as the network, must be managed centrally. This requirement is part of many regulatory frameworks. It's standard practice for any organization that grants or denies access to confidential or critical business resources.
  - Managing application resources that don't violate security boundaries or other aspects required to maintain security and compliance can be delegated to application teams. Allowing users to provision resources within a securely managed environment allows organizations to take advantage of the agile nature of the cloud while preventing the violation of any critical security or governance boundary.

### Design recommendations:

- Use Azure AD [RBAC](#) to manage data-plane access to resources, where possible. Examples are Azure Key Vault, a storage account, or a SQL database.
- Deploy Azure AD conditional-access policies for any user with rights to Azure environments. Doing so provides another mechanism to help protect a controlled Azure environment from unauthorized access.
- Enforce multi-factor authentication (MFA) for any user with rights to the Azure environments. MFA enforcement is a requirement of many compliance frameworks. It greatly lowers the risk of credential theft and unauthorized access.
- Use [Azure AD Privileged Identity Management \(PIM\)](#) to establish zero standing access and least privilege. Map your organization's roles to the minimum level of access needed. Azure AD PIM can either be an extension of existing tools and processes, use Azure

native tools as outlined, or use both as needed.

- Use Azure-AD-only groups for Azure control-plane resources in Azure AD PIM when you grant access to resources.
  - Add on-premises groups to the Azure-AD-only group if a group management system is already in place.
- Use Azure AD PIM access reviews to periodically validate resource entitlements. Access reviews are part of many compliance frameworks. As a result, many organizations will already have a process in place to address this requirement.
- Integrate Azure AD logs with the platform-central [Azure Monitor](#). Azure Monitor allows for a single source of truth around log and monitoring data in Azure, which gives organizations cloud-native options to meet requirements around log collection and retention.
- If any data sovereignty requirements exist, custom user policies can be deployed to enforce them.
- Use custom RBAC role definitions within the Azure AD tenant while you consider the following key roles:

ROLE	USAGE	ACTIONS	NO ACTIONS
Azure platform owner (i.e. Built-in Owner Role)	Management group and subscription lifecycle management	*	
Network management (NetOps)	Platform-wide global connectivity management: Virtual networks, UDRs, NSGs, NVAs, VPN, Azure ExpressRoute, and others	<pre>*/read, Microsoft.Authorization/*/write , Microsoft.Network/vpnGateways/* , Microsoft.Network/expressRouteCircuits/* , Microsoft.Network/routeTables/write , Microsoft.Network/vpnSites/*</pre>	
Security operations (SecOps)	Security administrator role with a horizontal view across the entire Azure estate and the Azure Key Vault purge policy	<pre>*/read, */register/action, Microsoft.KeyVault/locations/deletedVaults/purge/action , Microsoft.Insights/alertRules/* , Microsoft.Authorization/policyDefinitions/* , Microsoft.Authorization/policyAssignments/* , Microsoft.Authorization/policySetDefinitions/* , Microsoft.PolicyInsights/* , Microsoft.Security/*</pre>	
Subscription owner	Delegated role for subscription owner derived from subscription owner role	*	<pre>Microsoft.Authorization/*/write , Microsoft.Network/vpnGateways/* , Microsoft.Network/expressRouteCircuits/* , Microsoft.Network/routeTables/write , Microsoft.Network/vpnSites/*</pre>
Application owners (DevOps/AppOps)	Contributor role granted for application/operations team at resource group level		<pre>Microsoft.Network/publicIPAddresses/write , Microsoft.Network/virtualNetworks/write , Microsoft.KeyVault/locations/deletedVaults/purge/action</pre>

- Use Azure Security Center just-in-time access for all infrastructure as a service (IaaS) resources to enable network-level protection for ephemeral user access to IaaS virtual machines.
- Use Azure-AD-managed identities for Azure resources to avoid authentication based on user names and passwords. Because many security breaches of public cloud resources originate with credential theft embedded in code or other text sources, enforcing managed identities for programmatic access greatly reduces the risk of credential theft.
- Use privileged identities for automation runbooks that require elevated access permissions. Automated workflows that violate critical security boundaries should be governed by the same tools and policies users of equivalent privilege are.
- Don't add users directly to Azure resource scopes. Instead add users to defined roles, which are then assigned to resource scopes. Direct user assignments circumvent centralized management, greatly increasing the management required to prevent unauthorized access to restricted data.

#### Plan for authentication inside a landing zone

A critical design decision that an enterprise organization must make when adopting Azure is whether to extend an existing on-premises

identity domain into Azure or to create a brand new one. Requirements for authentication inside the landing zone should be thoroughly assessed and incorporated into plans to deploy Active Directory Domain Services (AD DS) in Windows server, Azure AD Domain Services (Azure AD DS), or both. Most Azure environments will use at least Azure AD for Azure fabric authentication and AD DS local host authentication and group policy management.

#### Design considerations:

- Consider centralized and delegated responsibilities to manage resources deployed inside the landing zone.
- Applications that rely on domain services and use older protocols can use [Azure AD DS](#).

#### Design recommendations:

- Use centralized and delegated responsibilities to manage resources deployed inside the landing zone based on role and security requirements.
- Privileged operations such as creating service principal objects, registering applications in Azure AD, and procuring and handling certificates or wildcard certificates require special permissions. Consider which users will be handling such requests and how to secure and monitor their accounts with the degree of diligence required.
- If an organization has a scenario where an application that uses integrated Windows authentication must be accessed remotely through Azure AD, consider using [Azure AD Application Proxy](#).
- There's a difference between Azure AD, Azure AD DS, and AD DS running on Windows server. Evaluate your application needs, and understand and document the authentication provider that each one will be using. Plan accordingly for all applications.
- Evaluate the compatibility of workloads for AD DS on Windows server and for Azure AD DS.
- Ensure your network design allows resources that require AD DS on Windows server for local authentication and management to access the appropriate domain controllers.
  - For AD DS on Windows server, consider shared services environments that offer local authentication and host management in a larger enterprise-wide network context.
- Deploy Azure AD DS within the primary region because this service can only be projected into one subscription.
- Use managed identities instead of service principals for authentication to Azure services. This approach reduces exposure to credential theft.

# Management group and subscription organization

11/9/2020 • 8 minutes to read • [Edit Online](#)

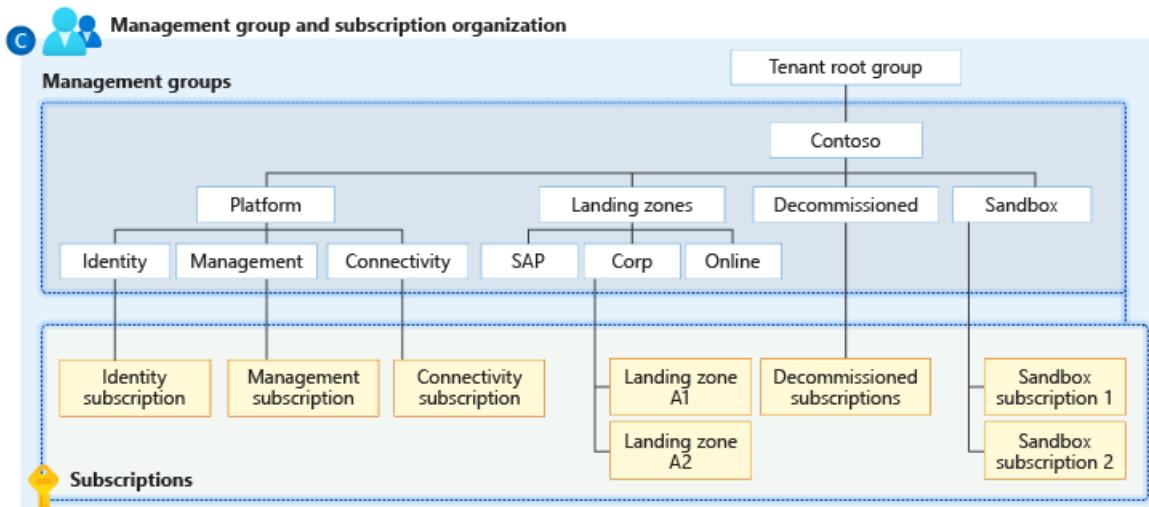


Figure 1: Management group hierarchy.

## Define a management group hierarchy

Management group structures within an Azure Active Directory (Azure AD) tenant support organizational mapping and must be considered thoroughly when an organization plans Azure adoption at scale.

### Design considerations:

- Management groups can be used to aggregate policy and initiative assignments via Azure Policy.
- A management group tree can support up to [six levels of depth](#). This limit doesn't include the tenant root level or the subscription level.
- Any principal (user, service principal) within an Azure AD tenant can create new management groups as RBAC authorization for management group operations is not enabled by default.
- All new subscription will be placed under the root management group by default.

### Design recommendations:

- Keep the management group hierarchy reasonably flat with no more than three to four levels, ideally. This restriction reduces management overhead and complexity.
- Avoid duplicating your organizational structure into a deeply nested management group hierarchy. Management groups should be used for policy assignment versus billing purposes. This approach necessitates using management groups for their intended purpose in enterprise-scale architecture, which is providing Azure policies for workloads that require the same type of security and compliance under the same management group level.
- Create management groups under your root-level management group to represent the types of workloads (archetype) that you'll host and ones based on their security, compliance, connectivity, and feature needs. This grouping structure allows you to have a set of Azure policies applied at the management group level for all workloads that require the same security, compliance, connectivity, and feature settings.
- Use resource tags, which can be enforced or appended through Azure Policy, to query and horizontally navigate across the management group hierarchy. Then you can group resources for search needs without having to use a complex management group hierarchy.
- Create a top-level sandbox management group to allow users to immediately experiment with Azure. Users can

then experiment with resources that might not yet be allowed in production environments. The sandbox provides isolation from your development, test, and production environments.

- For further guidance of the top-level sandbox management group review the [implementation guidelines](#).
- Use a dedicated service principal name (SPN) to execute management group management operations, subscription management operations, and role assignment. Using an SPN reduces the number of users who have elevated rights and follows least-privilege guidelines.
- Assign the `User Access Administrator` Azure role-based access control (RBAC) role at the root management group scope (`/`) to grant the SPN just mentioned access at the root level. After the SPN is granted permissions, the `User Access Administrator` role can be safely removed. In this way, only the SPN is part of the `User Access Administrator` role.
- Assign `Contributor` permission to the SPN previously mentioned at the root management group scope (`/`), which allows tenant-level operations. This permission level ensures that the SPN can be used to deploy and manage resources to any subscription within your organization.
- Create a `Platform` management group under the root management group to support common platform policy and RBAC assignment. This grouping structure ensures that different policies can be applied to the subscriptions used for your Azure foundation. It also ensures that the billing for common resources is centralized in one set of foundational subscriptions.
- Limit the number of Azure Policy assignments made at the root management group scope (`/`). This limitation minimizes debugging inherited policies in lower-level management groups.
- Ensure only privileged users can operate management groups in the tenant by enabling RBAC authorization in the management group hierarchy settings.
- Configure a default, dedicated management group for new subscriptions to ensure no subscriptions are placed under the root management group.

## Subscription organization and governance

Subscriptions are a unit of management, billing, and scale within Azure. They play a critical role when you're designing for large-scale Azure adoption. This section helps you capture subscription requirements and design target subscriptions based on critical factors. These factors are environment type, ownership and governance model, organizational structure, and application portfolios.

### Design considerations:

- Subscriptions serve as boundaries for assigning Azure policies. For example, secure workloads such as payment card industry (PCI) workloads typically require additional policies to achieve compliance. Instead of using a management group to group workloads that require PCI compliance, you can achieve the same isolation with a subscription. This way, you don't have too many management groups with a small number of subscriptions.
- Subscriptions serve as a scale unit so that component workloads can scale within the platform [subscription limits](#). Make sure to consider subscription resource limits during your workload design sessions.
- Subscriptions provide a management boundary for governance and isolation, which creates a clear separation of concerns.
- There's a manual process, planned future automation, that can be conducted to limit an Azure AD tenant to use only Enterprise Agreement enrollment subscriptions. This process prevents creation of Microsoft Developer Network subscriptions at the root management group scope.

### Design recommendations:

- Treat subscriptions as a democratized unit of management aligned with business needs and priorities.
- Make subscription owners aware of their roles and responsibilities:
  - Perform an access review in Azure AD Privileged Identity Management quarterly or twice a year to

- ensure that privileges don't proliferate as users move within the customer organization.
- Take full ownership of budget spending and resource utilization.
  - Ensure policy compliance and remediate when necessary.
  - Use the following principles when identifying requirements for new subscriptions:
    - **Scale limits:** Subscriptions serve as a scale unit for component workloads to scale within platform subscription limits. For example, large, specialized workloads such as high-performance computing, IoT, and SAP are all better suited to use separate subscriptions to avoid limits (such as a limit of 50 Azure Data Factory integrations).
    - **Management boundary:** Subscriptions provide a management boundary for governance and isolation, which allows for a clear separation of concerns. For example, different environments such as development, test, and production are often isolated from a management perspective.
    - **Policy boundary:** Subscriptions serve as a boundary for the assignment of Azure policies. For example, secure workloads such as PCI typically require additional policies to achieve compliance. This additional overhead doesn't need to be considered holistically if a separate subscription is used. Similarly, development environments might have more relaxed policy requirements relative to production environments.
    - **Target network topology:** Virtual networks can't be shared across subscriptions, but they can connect with different technologies such as virtual network peering or Azure ExpressRoute. Consider which workloads must communicate with each other when you decide whether a new subscription is required.
  - Group subscriptions together under management groups aligned within the management group structure and policy requirements at scale. Grouping ensures that subscriptions with the same set of policies and RBAC assignments can inherit them from a management group, which avoids duplicate assignments.
  - Establish a dedicated management subscription in the **Platform** management group to support global management capabilities such as Azure Monitor Log Analytics workspaces and Azure Automation runbooks.
  - Establish a dedicated identity subscription in the **Platform** management group to host Windows server Active Directory domain controllers, when necessary.
  - Establish a dedicated connectivity subscription in the **Platform** management group to host an Azure Virtual WAN hub, private Domain Name System (DNS), ExpressRoute circuit, and other networking resources. A dedicated subscription ensures that all foundation network resources are billed together and isolated from other workloads.
  - Avoid a rigid subscription model, and opt instead for a set of flexible criteria to group subscriptions across the organization. This flexibility ensures that as your organization's structure and workload composition changes, you can create new subscription groups instead of using a fixed set of existing subscriptions. One size doesn't fit all for subscriptions. What works for one business unit might not work for another. Some apps might coexist within the same landing zone subscription while others might require their own subscription.

## Configure subscription quota and capacity

Each Azure region contains a finite number of resources. When you consider an enterprise-scale Azure adoption that involves large resource quantities, ensure that sufficient capacity and SKUs are available and the attained capacity can be understood and monitored.

### Design considerations:

- Consider limits and quotas within the Azure platform for each service that your workloads require.
- Consider the availability of required SKUs within chosen Azure regions. For example, new features might be available only in certain regions. The availability of certain SKUs for given resources such as VMs might be different from one region to another.
- Consider that subscription quotas aren't capacity guarantees and are applied on a per-region basis.

### Design recommendations:

- Use subscriptions as scale units, and scale out resources and subscriptions as required. Your workload can then use the required resources for scaling out, when needed, without hitting subscription limits in the Azure platform.
- Use reserved instances to prioritize reserved capacity in required regions. Then your workload will have the required capacity even when there's a high demand for that resource in a specific region.
- Establish a dashboard with custom views to monitor used capacity levels. Set up alerts if capacity utilization is reaching critical levels (for example, 90 percent CPU utilization).
- Raise support requests for quota increase as a part of subscription provisioning (for example, total available VM cores within a subscription). This approach ensures your quota limits are set before your workloads require going over the default limits.
- Ensure required services and features are available within the chosen deployment regions.

## Establish cost management

Cost transparency across a technical estate is a critical management challenge faced by every large enterprise organization. This section explores key aspects associated with how cost transparency can be achieved across large Azure environments.

### Design considerations:

- Potential need for chargeback models where shared platform as a service (PaaS) resources are concerned, such as Azure App Service Environment and Azure Kubernetes Service, which might need to be shared to achieve higher density.
- Use a shutdown schedule for nonproduction workloads to optimize costs.
- Use Azure Advisor to check cost optimization recommendations.

### Design recommendations:

- Use Azure Cost Management and Billing for cost aggregation. Make it available to application owners.
- Use Azure resource tags for cost categorization and resource grouping. Using tags allows you to have a chargeback mechanism for workloads that share a subscription or for a given workload that spans across multiple subscriptions.

# Network topology and connectivity

11/9/2020 • 26 minutes to read • [Edit Online](#)

This article examines key design considerations and recommendations surrounding networking and connectivity to, from, and within Microsoft Azure.

## Plan for IP addressing

It's vital that your organization plans for IP addressing in Azure to ensure that IP address space doesn't overlap across on-premises locations and Azure regions.

### Design considerations:

- Overlapping IP address spaces across on-premises and Azure regions will create major contention challenges.
- You can add address space after you create a virtual network. This process requires an outage if the virtual network is already connected to another virtual network via virtual network peering because the peering must be deleted and re-created.
- Azure reserves five IP addresses within each subnet. Factor in those addresses when you're sizing virtual networks and encompassed subnets.
- Some Azure services require [dedicated subnets](#). These services include Azure Firewall and Azure VPN Gateway.
- You can delegate subnets to certain services to create instances of a service within the subnet.

### Design recommendations:

- Plan for non-overlapping IP address spaces across Azure regions and on-premises locations well in advance.
- Use IP addresses from the address allocation for private internets (RFC 1918).
- For environments that have limited availability of private IP addresses (RFC 1918), consider using IPv6.
- Don't create unnecessarily large virtual networks (for example, `/16`) to ensure that IP address space isn't wasted.
- Don't create virtual networks without planning the required address space in advance. Adding address space will cause an outage after a virtual network is connected via virtual network peering.
- Don't use public IP addresses for virtual networks, especially if the public IP addresses don't belong to your organization.

## Configure DNS and name resolution for on-premises and Azure resources

Domain Name System (DNS) is a critical design topic in the overall enterprise-scale architecture. Some organizations might want to use their existing investments in DNS. Others might see cloud adoption as an opportunity to modernize their internal DNS infrastructure and use native Azure capabilities.

### Design considerations:

- You can use a DNS resolver in conjunction with Azure Private DNS for cross-premises name resolution.
- You might require the use of existing DNS solutions across on-premises and Azure.
- The maximum number of private DNS zones to which a virtual network can link with auto-registration is one.
- The maximum number of private DNS zones to which a virtual network can link is 1,000 without auto-registration enabled.

#### Design recommendations:

- For environments where name resolution in Azure is all that's required, use Azure Private DNS for resolution. Create a delegated zone for name resolution (such as `azure.contoso.com`).
- For environments where name resolution across Azure and on-premises is required, use existing DNS infrastructure (for example, Active Directory integrated DNS) deployed onto at least two Azure virtual machines (VMs). Configure DNS settings in virtual networks to use those DNS servers.
- You can still link an Azure Private DNS zone to the virtual networks and use DNS servers as hybrid resolvers with conditional forwarding to on-premises DNS names, such as `onprem.contoso.com`, by using on-premises DNS servers. You can configure on-premises servers with conditional forwarders to resolver VMs in Azure for the Azure Private DNS zone (for example, `azure.contoso.com`).
- Special workloads that require and deploy their own DNS (such as Red Hat OpenShift) should use their preferred DNS solution.
- Enable auto-registration for Azure DNS to automatically manage the lifecycle of the DNS records for the virtual machines deployed within a virtual network.
- Use a virtual machine as a resolver for cross-premises DNS resolution with Azure Private DNS.
- Create the Azure Private DNS zone within a global connectivity subscription. You might create other Azure Private DNS zones (for example, `privatelink.database.windows.net` or `privatelink.blob.core.windows.net` for Azure Private Link).

## Define an Azure network topology

Network topology is a critical element of the enterprise-scale architecture because it defines how applications can communicate with each other. This section explores technologies and topology approaches for enterprise Azure deployments. It focuses on two core approaches: topologies based on Azure Virtual WAN, and traditional topologies.

Use a network topology based on Azure Virtual WAN if any of the following are true:

- Your organization intends to deploy resources across several Azure regions and needs to connect your global locations to both Azure and on-premises.
- Your organization intends to use software-defined WAN (SD-WAN) deployments fully integrated with Azure.
- You intend to deploy up to 2,000 virtual machine workloads across all VNets connected to a single Azure Virtual WAN hub.

Virtual WAN is used to meet large-scale interconnectivity requirements. Because it's a Microsoft-managed service, it also reduces overall network complexity and helps to modernize your organization's network.

Use a traditional Azure network topology if any of the following are true:

- Your organization intends to deploy resources across several Azure regions.
- You can use global VNet peering to connect virtual networks across Azure regions.

- You have a low number of remote or branch locations per region. That is, you need fewer than 30 IP security (IPsec) tunnels.
- You require full control and granularity for manually configuring your Azure network.

A traditional network topology helps you build a secure large-scale network in Azure.

## Virtual WAN network topology (Microsoft-managed)

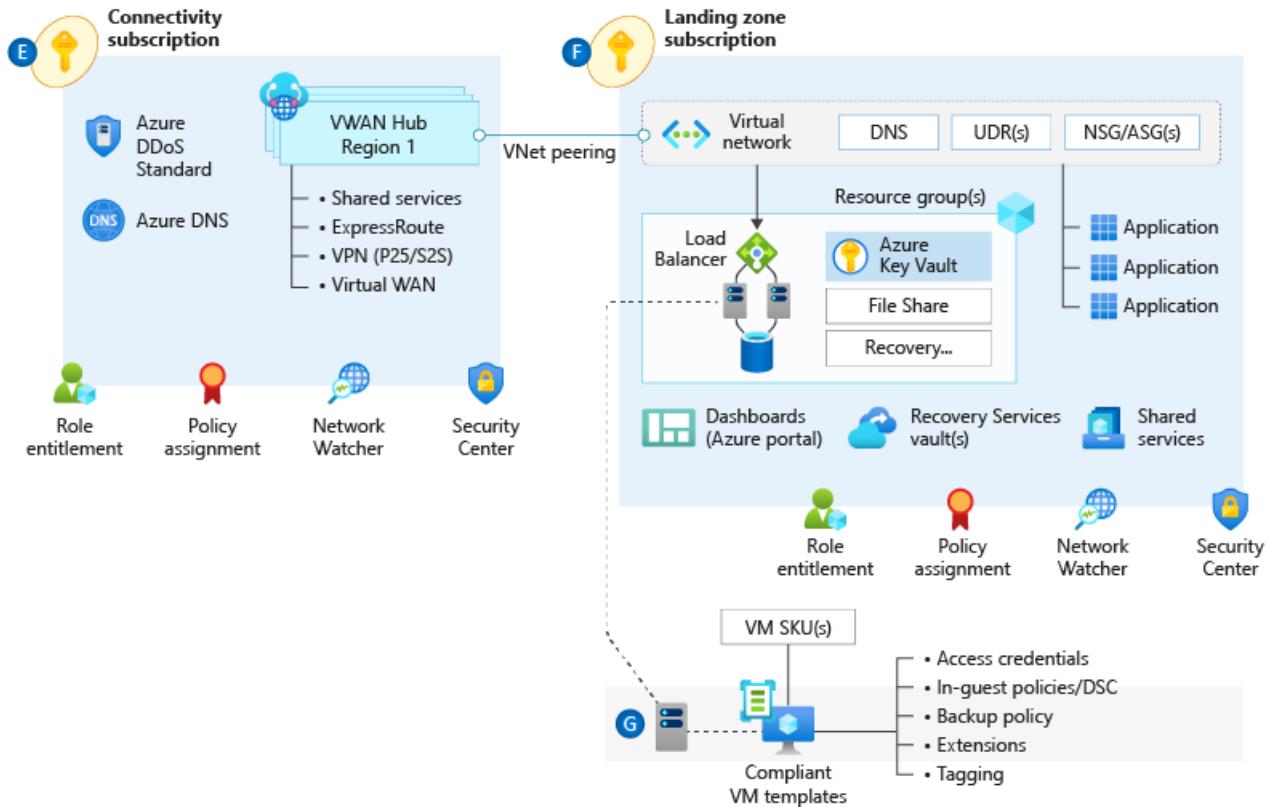


Figure 1: Virtual WAN network topology.

### Design considerations:

- **Azure Virtual WAN** is a Microsoft-managed solution that provides end-to-end global transit connectivity by default. Virtual WAN hubs eliminate the need to manually configure network connectivity. For example, you don't need to set up user-defined routing (UDR) or network virtual appliances (NVAs) to enable global transit connectivity.
- Virtual WAN greatly simplifies end-to-end network connectivity in Azure and cross-premises by creating a **hub-and-spoke network architecture**. The architecture spans multiple Azure regions and on-premises locations (any-to-any connectivity) out of the box, as shown in this figure:

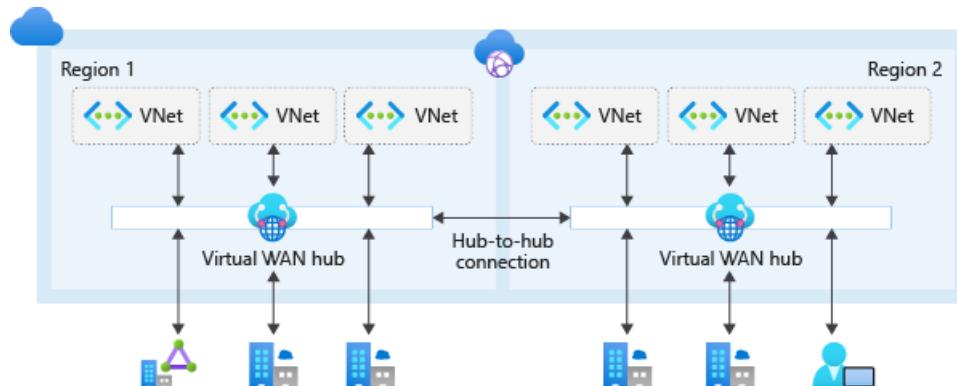


Figure 2: Global transit network with Virtual WAN.

- Virtual WAN any-to-any transitive connectivity supports the following paths (within the same region and across regions):
  - Virtual network to virtual network
  - Virtual network to branch
  - Branch to virtual network
  - Branch to branch
- Virtual WAN hubs are locked down. The only resources that you can deploy within them are virtual network gateways (point-to-site VPN, site-to-site VPN, and Azure ExpressRoute), Azure Firewall via Firewall Manager, and route tables.
- Virtual WAN increases the limit of up to 200 prefixes advertised from Azure to on-premises via ExpressRoute private peering to 10,000 prefixes per Virtual WAN hub. The limit of 10,000 prefixes also includes site-to-site VPN and point-to-site VPN.
- Network-to-network transitive connectivity (within a region and across regions) is now in general availability (GA).
- Virtual WAN hub-to-hub connectivity is now in GA.
- Transit connectivity between the virtual networks in Standard Virtual WAN is enabled due to the presence of a router in every virtual hub. Every virtual hub router supports an aggregate throughput up to 50 Gbps.
- A maximum of 2,000 VM workloads across all VNets can be connected to a single Virtual WAN hub.
- Virtual WAN integrates with a variety of [SD-WAN providers](#).
- Many managed service providers offer [managed services](#) for Virtual WAN.
- VPN gateways in Virtual WAN can scale up to 20 Gbps and 20,000 connections per virtual hub.
- ExpressRoute circuits with the premium add-on are required. They should be from an ExpressRoute Global Reach location.
- Azure Firewall Manager, now in GA, allows the deployment of Azure Firewall in the Virtual WAN hub.
- Virtual WAN hub-to-hub traffic via Azure Firewall is currently not supported. As alternative, use the native hub-to-hub transit routing capabilities in Virtual WAN. Use network security groups (NSGs) to allow or block virtual network traffic across hubs.

#### **Design recommendations:**

- We recommend Virtual WAN for new large or global network deployments in Azure where you need global transit connectivity across Azure regions and on-premises locations. That way, you don't have to manually set up transitive routing for Azure networking.

The following figure shows a sample global enterprise deployment with datacenters spread across Europe and the United States. The deployment also has a large number of branch offices within both regions. The environment is globally connected via Virtual WAN and ExpressRoute Global Reach.

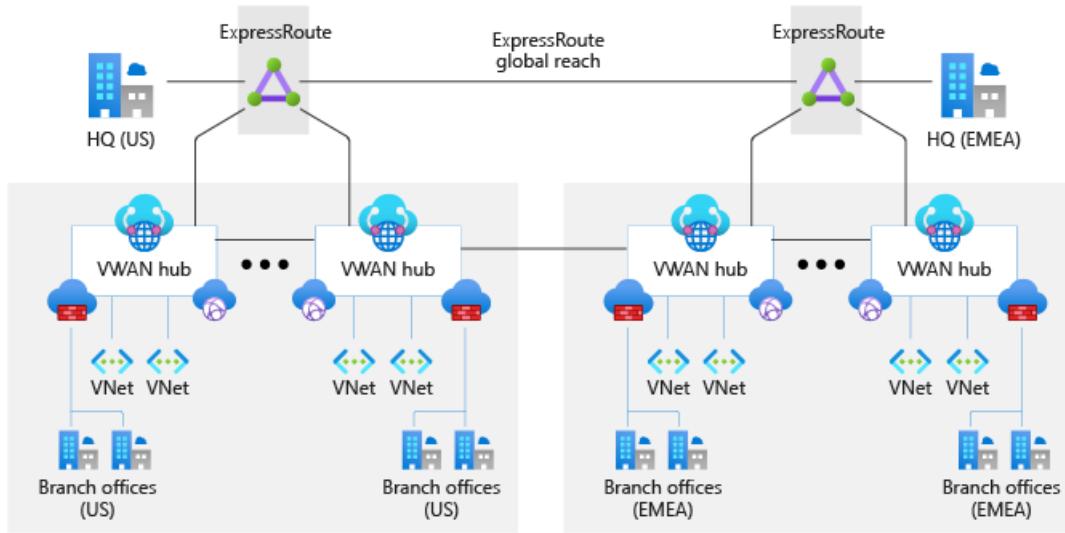


Figure 3: Sample network topology.

- Use Virtual WAN as a global connectivity resource. Use a Virtual WAN hub per Azure region to connect multiple landing zones together across Azure regions via the local Virtual WAN hub.
- Connect Virtual WAN hubs to on-premises datacenters by using ExpressRoute.
- Deploy required shared services, like DNS servers, in a dedicated landing zone. Required shared resources can't be deployed on a Virtual WAN hub.
- Connect branches and remote locations to the nearest Virtual WAN hub via site-to-site VPN, or enable branch connectivity to Virtual WAN via an SD-WAN partner solution.
- Connect users to the Virtual WAN hub via a point-to-site VPN.
- Follow the principle "traffic in Azure stays in Azure" so that communication across resources in Azure occurs via the Microsoft backbone network, even when the resources are in different regions.
- Deploy Azure Firewall in Virtual WAN hubs for east/west and south/north traffic protection and filtering within an Azure region.
- If partner NVAs are required for east/west or south/north traffic protection and filtering, deploy the NVAs to a separate virtual network such as an NVA virtual network. Connect it to the regional Virtual WAN hub and to the landing zones that need access to NVAs. For more information, see [Create a Virtual WAN hub route table for NVAs](#).
- When you're deploying partner networking technologies and NVAs, follow the partner vendor's guidance to ensure there are no conflicting configurations with Azure networking.
- Don't build a transit network on top of Azure Virtual WAN. Virtual WAN satisfies transitive network topology requirements such as the ability to use third-party NVAs. Building a transit network on top of Azure Virtual WAN would be redundant and increase complexity.
- Don't use existing on-premises networks like multiprotocol label switching (MPLS) to connect Azure resources across Azure regions, as Azure networking technologies support the interconnection of Azure resources across regions through the Microsoft backbone. This is because of the performance and uptime characteristics of the Microsoft backbone as well as routing simplicity. This suggestion addresses the performance and uptime characteristics of the Microsoft backbone. It also encourages routing simplicity.
- For brownfield scenarios where you're migrating from a hub-and-spoke network topology not based on Virtual WAN, see [Migrate to Azure Virtual WAN](#).
- Create Azure Virtual WAN and Azure Firewall resources within the connectivity subscription.

- Don't create more than 500 virtual network connections per Virtual WAN virtual hub.
- Plan your deployment carefully, and ensure that your network architecture is within the [Azure Virtual WAN limits](#).

## Traditional Azure networking topology

Although Virtual WAN offers a wide range of powerful capabilities, a traditional Azure networking approach might be optimal in some cases:

- If a global transitive network across multiple Azure regions or cross-premises isn't required. An example is a branch in the United States that requires connectivity to a virtual network in Europe.
- If you need to deploy a global network across multiple Azure regions, and you can use global VNet peering to connect virtual networks across regions.
- If there's no need to connect to a large number of remote locations via VPN or integration with an SD-WAN solution.
- If your organization's preference is to have granular control and configuration when setting up a network topology in Azure.

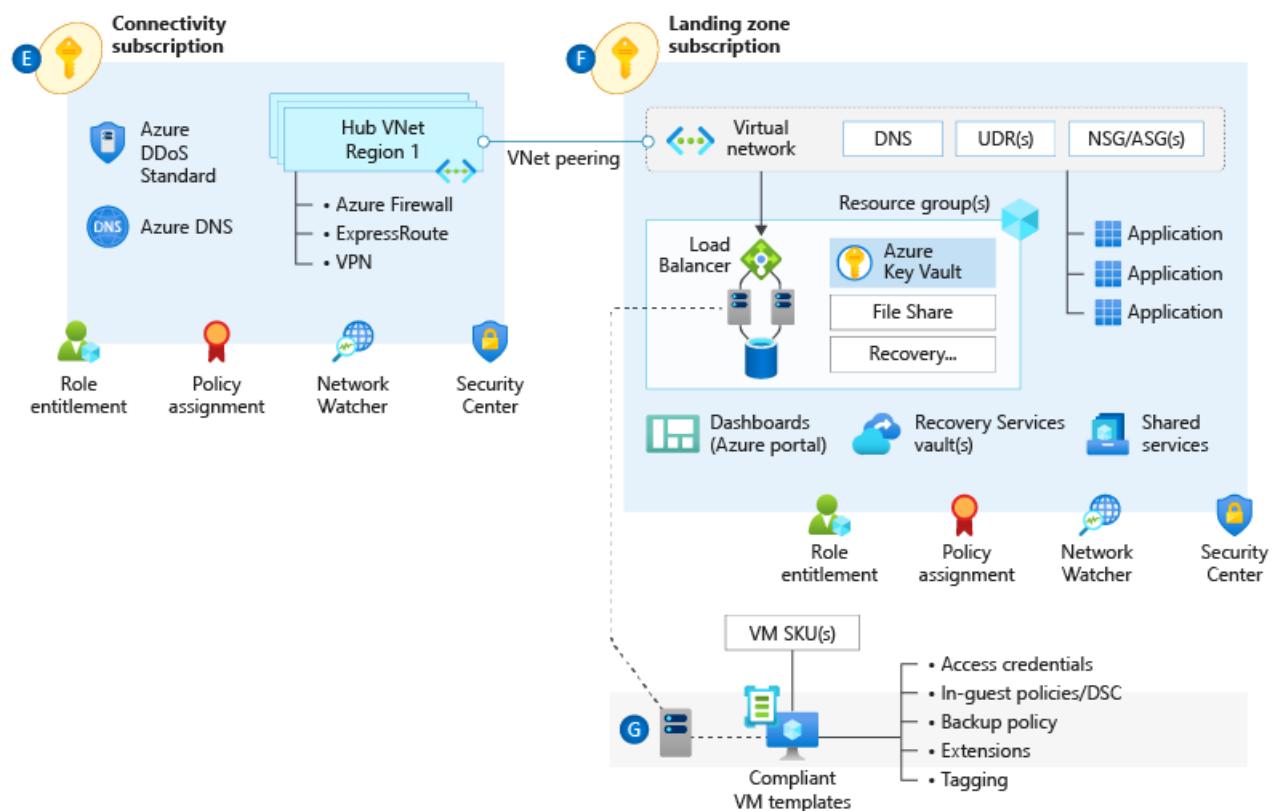


Figure 4: A traditional Azure network topology.

### Design considerations:

- Various network topologies can connect multiple landing zone virtual networks. Examples are one large flat virtual network, multiple virtual networks connected with multiple ExpressRoute circuits or connections, hub and spoke, full mesh, and hybrid.
- Virtual networks don't traverse subscription boundaries. But, you can achieve connectivity between virtual networks in different subscriptions by using virtual network peering, an ExpressRoute circuit, or VPN gateways.
- You can use virtual network peering to connect virtual networks in the same region, across different Azure regions, and across different Azure Active Directory (Azure AD) tenants.

- Virtual network peering and global virtual network peering aren't transitive. UDRs and NVAs are required to enable a transit network. For more information, see [Hub-spoke network topology in Azure](#).
- You can use ExpressRoute circuits to establish connectivity across virtual networks within the same geopolitical region or by using the premium add-on for connectivity across geopolitical regions. Keep these points in mind:
  - Network-to-network traffic might experience more latency because traffic must hairpin at the Microsoft enterprise edge (MSEE) routers.
  - Bandwidth will be constrained to the ExpressRoute gateway SKU.
  - You must still deploy and manage UDRs if they require inspection or logging for traffic across virtual networks.
- VPN gateways with Border Gateway Protocol (BGP) are transitive within Azure and on-premises, but they don't transit across ExpressRoute gateways.
- When multiple ExpressRoute circuits are connected to the same virtual network, use connection weights and BGP techniques to ensure an optimal path for traffic between on-premises and Azure. For more information, see [Optimize ExpressRoute routing](#).
- Using BGP techniques to influence ExpressRoute routing is a configuration outside the Azure platform. Your organization or your connectivity provider must configure the on-premises routers accordingly.
- ExpressRoute circuits with premium add-ons provide global connectivity. However, the maximum number of ExpressRoute connections per ExpressRoute gateway is four.
- Although the maximum number of virtual network peering connections per virtual network is 500, the maximum number of routes that can be advertised from Azure to on-premises via ExpressRoute private peering is 200.
- A VPN gateway's maximum aggregated throughput is 10 Gbps. It supports up to 30 site-to-site or network-to-network tunnels.

#### **Design recommendations:**

- Consider a network design based in the hub-and-spoke network topology with non-Virtual WAN technologies for the following scenarios:
  - The traffic boundary in an Azure deployment is within an Azure region.
  - A network architecture spans multiple Azure regions, and there's no need for transitive connectivity between virtual networks for landing zones across regions.
  - A network architecture spans multiple Azure regions, and global VNet peering can be used to connect virtual networks across Azure regions.
  - There's no need for transitive connectivity between VPN and ExpressRoute connections.
  - The main cross-premises connectivity channel is ExpressRoute, and the number of VPN connections is less than 30 per VPN gateway.
  - There's a dependency on centralized NVAs and granular routing.
- For regional deployments, primarily use the hub-and-spoke topology. Use landing-zone virtual networks that connect with virtual network peering to a central-hub virtual network for cross-premises connectivity via ExpressRoute, VPN for branch connectivity, spoke-to-spoke connectivity via NVAs and UDRs, and internet-outbound protection via NVA. The following figure shows this topology. This allows for appropriate traffic control to meet most requirements for segmentation and inspection.

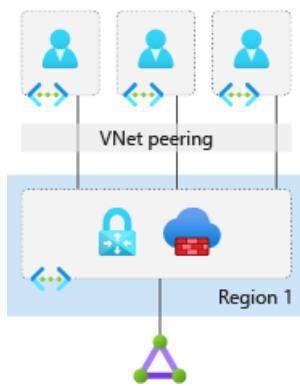


Figure 5: Hub-and-spoke network topology.

- Use the topology of multiple virtual networks connected with multiple ExpressRoute circuits when one of these conditions is true:
  - You need a high level of isolation.
  - You need dedicated ExpressRoute bandwidth for specific business units.
  - You've reached the maximum number of connections per ExpressRoute gateway (up to four).

The following figure shows this topology.

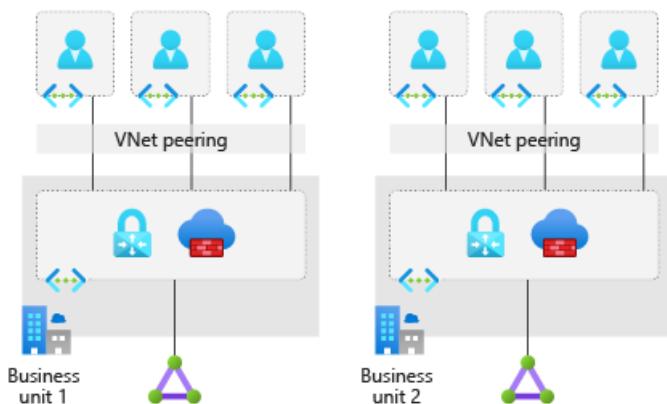
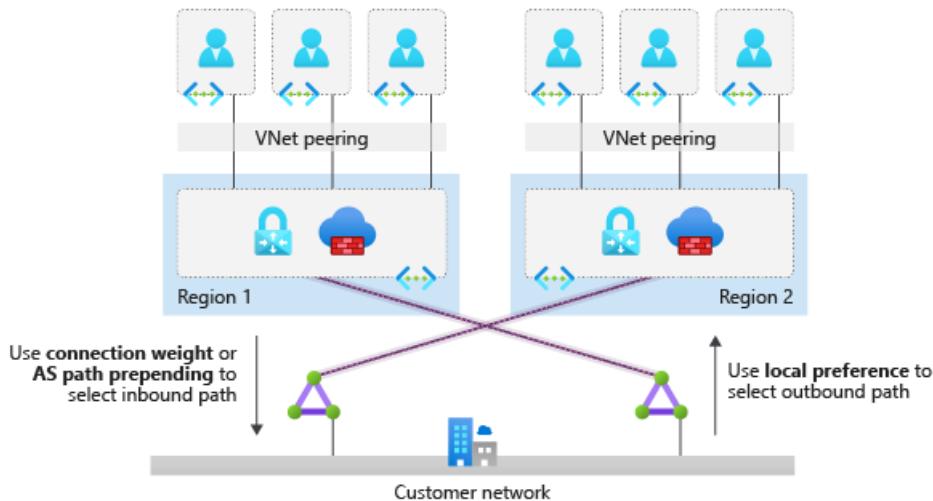


Figure 6: Multiple virtual networks connected with multiple ExpressRoute circuits.

- Deploy a set of minimal shared services, including ExpressRoute gateways, VPN gateways (as required), and Azure Firewall or partner NVAs (as required) in the central-hub virtual network. If necessary, also deploy Active Directory domain controllers and DNS servers.
- Deploy Azure Firewall or partner NVAs for east/west or south/north traffic protection and filtering, in the central-hub virtual network.
- When you're deploying partner networking technologies or NVAs, follow the partner vendor's guidance to ensure that:
  - The vendor supports deployment.
  - The guidance is designed for high availability and maximal performance.
  - There are no conflicting configurations with Azure networking.
- Don't deploy L7 inbound NVAs such as Azure Application Gateway as a shared service in the central-hub virtual network. Instead, deploy them together with the app in their respective landing zones.
- Use your existing network, MPLS and SD-WAN, for connecting branch locations with corporate headquarters. Transit in Azure between ExpressRoute and VPN gateways isn't supported.
- For network architectures with multiple hub-and-spoke topologies across Azure regions, use global virtual

network peering to connect landing-zone virtual networks when a small number of landing zones need to communicate across regions. This approach offers benefits like high network bandwidth with global virtual network peering, as allowed by the VM SKU. But it will bypass the central NVA, in case traffic inspection or filtering is required. This would also be subject to [limitations on global virtual network peering](#).

- When you deploy a hub-and-spoke network architecture in two Azure regions and transit connectivity between all landing zones across regions is required, use ExpressRoute with dual circuits to provide transit connectivity for landing-zone virtual networks across Azure regions. In this scenario, landing zones can transit within a region via NVA in local-hub virtual network and across regions via ExpressRoute circuit. Traffic must hairpin at the MSEE routers. The following figure shows this design.



*Figure 7: Landing zone connectivity design.*

- When your organization requires hub-and-spoke network architectures across more than two Azure regions and global transit connectivity between landing zones, virtual networks across Azure regions are required. You can implement this architecture by interconnecting central-hub virtual networks with global virtual network peering and using UDRs and NVAs to enable global transit routing. Because the complexity and management overhead are high, we recommend evaluating a global transit network architecture with Virtual WAN.
- Use [Azure Monitor for Networks \(Preview\)](#) to monitor the end-to-end state of your networks on Azure.
- Don't create more than 200 peering connections per central-hub virtual network. Although virtual networks support up to 500 peering connections, ExpressRoute with private peering only supports advertising up to 200 prefixes from Azure to on-premises.

## Connectivity to Azure

This section expands on the network topology to consider recommended models for connecting on-premises locations to Azure.

### Design considerations:

- Azure ExpressRoute provides dedicated private connectivity to Azure infrastructure as a service (IaaS) and platform as a service (PaaS) functionality from on-premises locations.
- You can use Private Link to establish connectivity to PaaS services over ExpressRoute with private peering.
- When multiple virtual networks are connected to the same ExpressRoute circuit, they'll become part of the same routing domain, and all virtual networks will share the bandwidth.
- You can use ExpressRoute Global Reach, where available, to connect on-premises locations together through ExpressRoute circuits to transit traffic over the Microsoft backbone network.

- ExpressRoute Global Reach is available in many [ExpressRoute peering locations](#).
- ExpressRoute Direct allows creation of multiple ExpressRoute circuits at no additional cost, up to the ExpressRoute Direct port capacity (10 Gbps or 100 Gbps). It also allows you to connect directly to Microsoft's ExpressRoute routers. For the 100-Gbps SKU, the minimum circuit bandwidth is 5 Gbps. For the 10-Gbps SKU, the minimum circuit bandwidth is 1 Gbps.

#### **Design recommendations:**

- Use ExpressRoute as the primary connectivity channel for connecting an on-premises network to Azure. You can use VPNs as a source of backup connectivity to enhance connectivity resiliency.
- Use dual ExpressRoute circuits from different peering locations when you're connecting an on-premises location to virtual networks in Azure. This setup will ensure redundant paths to Azure by removing single points of failure between on-premises and Azure.
- When you use multiple ExpressRoute circuits, [optimize ExpressRoute routing via BGP local preference and AS PATH prepending](#).
- Ensure that you're using the right SKU for the ExpressRoute/VPN gateways based on bandwidth and performance requirements.
- Deploy a zone-redundant ExpressRoute gateway in the supported Azure regions.
- For scenarios that require bandwidth higher than 10 Gbps or dedicated 10/100-Gbps ports, use ExpressRoute Direct.
- When low latency is required, or throughput from on-premises to Azure must be greater than 10 Gbps, enable FastPath to bypass the ExpressRoute gateway from the data path.
- Use VPN gateways to connect branches or remote locations to Azure. For higher resilience, deploy zone-redundant gateways (where available).
- Use ExpressRoute Global Reach to connect large offices, regional headquarters, or datacenters connected to Azure via ExpressRoute.
- When traffic isolation or dedicated bandwidth is required, such as for separating production and nonproduction environments, use different ExpressRoute circuits. It will help you ensure isolated routing domains and alleviate noisy-neighbor risks.
- Proactively monitor ExpressRoute circuits by using Network Performance Monitor.
- Don't explicitly use ExpressRoute circuits from a single peering location. This creates a single point of failure and makes your organization susceptible to peering location outages.
- Don't use the same ExpressRoute circuit to connect multiple environments that require isolation or dedicated bandwidth, to avoid noisy-neighbor risks.

## Connectivity to Azure PaaS services

Building on the previous connectivity sections, this section explores recommended connectivity approaches for using Azure PaaS services.

#### **Design considerations:**

- Azure PaaS services are typically accessed over public endpoints. However, the Azure platform provides capabilities to secure such endpoints or even make them entirely private:
  - Virtual network injection provides dedicated private deployments for supported services. But management plane traffic flows through public IP addresses.

- [Private Link](#) provides dedicated access by using private IP addresses to Azure PaaS instances or custom services behind Azure Load Balancer Standard.
- Virtual network service endpoints provide service-level access from selected subnets to selected PaaS services.
- Enterprises often have concerns about public endpoints for PaaS services that must be appropriately mitigated.
- For [supported services](#), Private Link addresses data exfiltration concerns associated with service endpoints. As an alternative, you can use outbound filtering via NVAs to provide steps to mitigate data exfiltration.

#### **Design recommendations:**

- Use virtual network injection for supported Azure services to make them available from within your virtual network.
- Azure PaaS services that have been injected into a virtual network still perform management plane operations by using public IP addresses. Ensure that this communication is locked down within the virtual network by using UDRs and NSGs.
- Use Private Link, [where available](#), for shared Azure PaaS services. Private Link is generally available for several services and is in public preview for numerous ones.
- Access Azure PaaS services from on-premises via ExpressRoute private peering. Use either virtual network injection for dedicated Azure services or Azure Private Link for available shared Azure services. To access Azure PaaS services from on-premises when virtual network injection or Private Link isn't available, use ExpressRoute with Microsoft peering. This method avoids transiting over the public internet.
- Use virtual network service endpoints to secure access to Azure PaaS services from within your virtual network, but only when Private Link isn't available and there are no data exfiltration concerns. To address data exfiltration concerns with service endpoints, use NVA filtering or use virtual network service endpoint policies for Azure Storage.
- Don't enable virtual network service endpoints by default on all subnets.
- Don't use virtual network service endpoints when there are data exfiltration concerns, unless you use NVA filtering.
- We don't recommend that you implement forced tunneling to enable communication from Azure to Azure resources.

## **Plan for inbound and outbound internet connectivity**

This section describes recommended connectivity models for inbound and outbound connectivity to and from the public internet.

#### **Design considerations:**

- Azure-native network security services such as Azure Firewall, Azure Web Application Firewall (WAF) on Azure Application Gateway, and Azure Front Door Service are fully managed services. So you don't incur the operational and management costs associated with infrastructure deployments, which can become complex at scale.
- The enterprise-scale architecture is fully compatible with partner NVAs, if your organization prefers to use NVAs or for situations where native services don't satisfy your organization's specific requirements.

#### **Design recommendations:**

- Use Azure Firewall to govern:
  - Azure outbound traffic to the internet.
  - Non-HTTP/S inbound connections.
  - East/west traffic filtering (if your organization requires it).
- Use Firewall Manager with Virtual WAN to deploy and manage Azure firewalls across Virtual WAN hubs or in hub virtual networks. Firewall Manager is now in GA for both Virtual WAN and regular virtual networks.
- Create a global Azure Firewall policy to govern security posture across the global network environment and assign it to all Azure Firewall instances. Allow for granular policies to meet requirements of specific regions by delegating incremental firewall policies to local security teams via role-based access control.
- Configure supported partner SaaS security providers within Firewall Manager if your organization wants to use such solutions to help protect outbound connections.
- Use WAF within a landing-zone virtual network for protecting inbound HTTP/S traffic from the internet.
- Use Azure Front Door Service and WAF policies to provide global protection across Azure regions for inbound HTTP/S connections to a landing zone.
- When you're using Azure Front Door Service and Azure Application Gateway to help protect HTTP/S apps, use WAF policies in Azure Front Door Service. Lock down Azure Application Gateway to receive traffic only from Azure Front Door Service.
- If partner NVAs are required for east/west or south/north traffic protection and filtering:
  - For Virtual WAN network topologies, deploy the NVAs to a separate virtual network (for example, NVA virtual network). Then connect it to the regional Virtual WAN hub and to the landing zones that require access to NVAs. [This article](#) describes the process.
  - For non-Virtual WAN network topologies, deploy the partner NVAs in the central-hub virtual network.
- If partner NVAs are required for inbound HTTP/S connections, deploy them within a landing-zone virtual network and together with the apps that they're protecting and exposing to the internet.
- Use [Azure DDoS Protection Standard protection plans](#) to help protect all public endpoints hosted within your virtual networks.
- Don't replicate on-premises perimeter network concepts and architectures into Azure. Similar security capabilities are available in Azure, but the implementation and architecture must be adapted to the cloud.

## Plan for app delivery

This section explores key recommendations to deliver internal-facing and external-facing apps in a secure, highly scalable, and highly available way.

### Design considerations:

- Azure Load Balancer (internal and public) provides high availability for app delivery at a regional level.
- Azure Application Gateway allows the secure delivery of HTTP/S apps at a regional level.
- Azure Front Door Service allows the secure delivery of highly available HTTP/S apps across Azure regions.
- Azure Traffic Manager allows the delivery of global apps.

### Design recommendations:

- Perform app delivery within landing zones for both internal-facing and external-facing apps.

- For secure delivery of HTTP/S apps, use Application Gateway v2 and ensure that WAF protection and policies are enabled.
- Use a partner NVA if you can't use Application Gateway v2 for the security of HTTP/S apps.
- Deploy Azure Application Gateway v2 or partner NVAs used for inbound HTTP/S connections within the landing-zone virtual network and with the apps that they're securing.
- Use a DDoS standard protection plan for all public IP addresses in a landing zone.
- Use Azure Front Door Service with WAF policies to deliver and help protect global HTTP/S apps that span Azure regions.
- When you're using Azure Front Door Service and Application Gateway to help protect HTTP/S apps, use WAF policies in Azure Front Door Service. Lock down Application Gateway to receive traffic only from Azure Front Door Service.
- Use Traffic Manager to deliver global apps that span protocols other than HTTP/S.

## Plan for landing zone network segmentation

This section explores key recommendations to deliver highly secure internal network segmentation within a landing zone to drive a network zero-trust implementation.

### Design considerations:

- The zero-trust model assumes a breached state and verifies each request as though it originates from an uncontrolled network.
- An advanced zero-trust network implementation employs fully distributed ingress/egress cloud micro-perimeters and deeper micro-segmentation.
- Network security groups can use Azure service tags to facilitate connectivity to Azure PaaS services.
- App security groups don't span or provide protection across virtual networks.
- NSG flow logs are now supported through Azure Resource Manager templates.

### Design recommendations:

- Delegate subnet creation to the landing zone owner. This will enable them to define how to segment workloads across subnets (for example, a single large subnet, multitier app, or network-injected app). The platform team can use Azure Policy to ensure that an NSG with specific rules (such as deny inbound SSH or RDP from internet, or allow/block traffic across landing zones) is always associated with subnets that have deny-only policies.
- Use NSGs to help protect traffic across subnets, as well as east/west traffic across the platform (traffic between landing zones).
- The app team should use app security groups at the subnet-level NSGs to help protect multitier VMs within the landing zone.
- Use NSGs and app security groups to micro-segment traffic within the landing zone and avoid using a central NVA to filter traffic flows.
- Enable NSG flow logs and feed them into Traffic Analytics to gain insights into internal and external traffic flows.
- Use NSGs to selectively allow connectivity between landing zones.
- For Virtual WAN topologies, route traffic across landing zones via Azure Firewall if your organization

requires filtering and logging capabilities for traffic flowing across landing zones.

## Define network encryption requirements

This section explores key recommendations to achieve network encryption between on-premises and Azure as well as across Azure regions.

### Design considerations:

- Cost and available bandwidth are inversely proportional to the length of the encryption tunnel between endpoints.
- When you're using a VPN to connect to Azure, traffic is encrypted over the internet via IPsec tunnels.
- When you're using ExpressRoute with private peering, traffic isn't currently encrypted.
- Configuring a Site-to-Site VPN connection over ExpressRoute private peering is now in [preview](#).
- You can apply [media access control security \(MACsec\)](#) encryption to ExpressRoute Direct to achieve network encryption.
- When Azure traffic moves between datacenters (outside physical boundaries not controlled by Microsoft or on behalf of Microsoft), [MACsec data-link layer encryption](#) is utilized on the underlying network hardware. This is applicable to VNet peering traffic.

### Design recommendations:

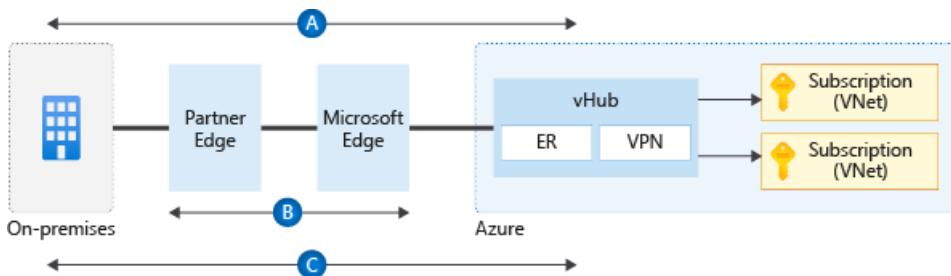


Figure 8: Encryption flows.

- When you're establishing VPN connections from on-premises to Azure by using VPN gateways, traffic is encrypted at a protocol level through IPsec tunnels. The preceding diagram shows this encryption in flow **A**.
- When you're using ExpressRoute Direct, configure [MACsec](#) in order to encrypt traffic at the layer-two level between your organization's routers and MSEE. The diagram shows this encryption in flow **B**.
- For Virtual WAN scenarios where MACsec isn't an option (for example, not using ExpressRoute Direct), use a Virtual WAN VPN gateway to establish [IPsec tunnels over ExpressRoute private peering](#). The diagram shows this encryption in flow **C**.
- For non-Virtual WAN scenarios, and where MACsec isn't an option (for example, not using ExpressRoute Direct), the only options are:
  - Use partner NVAs to establish IPsec tunnels over ExpressRoute private peering.
  - Establish a VPN tunnel over ExpressRoute with Microsoft peering.
  - Evaluate the capability to configure a Site-to-Site VPN connection over ExpressRoute private peering ([in preview](#)).
- If traffic between Azure regions must be encrypted, use Global VNet Peering to connect virtual networks across regions.
- If native Azure solutions (as shown in flows **B** and **C** in the diagram) don't meet your requirements, use

partner NVAs in Azure to encrypt traffic over ExpressRoute private peering.

## Plan for traffic inspection

In many industries, organizations require that traffic in Azure is mirrored to a network packet collector for deep inspection and analysis. This requirement typically focuses on inbound and outbound internet traffic. This section explores key considerations and recommended approaches for mirroring or tapping traffic within Azure Virtual Network.

### Design considerations:

- [Azure Virtual Network Terminal Access Point \(TAP\)](#) is in preview. Contact [azurevnettap@microsoft.com](mailto:azurevnettap@microsoft.com) for availability details.
- Packet capture in Azure Network Watcher is generally available, but captures are limited to a maximum period of five hours.

### Design recommendations:

As an alternative to Azure Virtual Network TAP, evaluate the following options:

- Use Network Watcher packets to capture despite the limited capture window.
- Evaluate if the latest version of NSG flow logs provides the level of detail that you need.
- Use partner solutions for scenarios that require deep packet inspection.
- Don't develop a custom solution to mirror traffic. Although this approach might be acceptable for small-scale scenarios, we don't encourage it at scale because of complexity and the supportability issues that might arise.

# Management and monitoring

11/9/2020 • 5 minutes to read • [Edit Online](#)

## Plan platform management and monitoring

This section explores how to operationally maintain an Azure enterprise estate with centralized management and monitoring at a platform level. More specifically, it presents key recommendations for central teams to maintain operational visibility within a large-scale Azure platform.

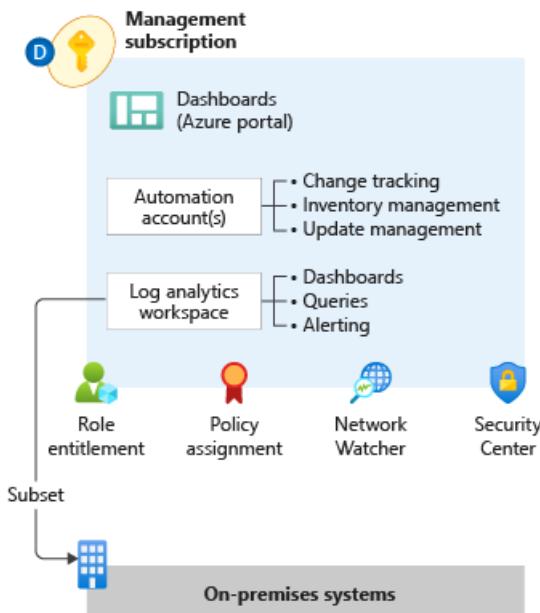


Figure 1: Platform management and monitoring.

### Design considerations:

- Use an Azure Monitor Log Analytics workspace as an administrative boundary.
- Application-centric platform monitoring, encompassing both hot and cold telemetry paths for metrics and logs, respectively:
  - Operating system metrics; for example, performance counters and custom metrics
  - Operating system logs; for example, Internet Information Services, Event Tracing for Windows, and syslogs
  - Resource health events
- Security audit logging and achieving a horizontal security lens across your organization's entire Azure estate:
  - Potential integration with on-premises security information and event management (SIEM) systems such as ServiceNow, ArcSight, or the Onapsis security platform
  - Azure activity logs
  - Azure Active Directory (Azure AD) audit reports
  - Azure diagnostic services, logs, and metrics; Azure Key Vault audit events; network security group (NSG) flow logs; and event logs
  - Azure Monitor, Azure Network Watcher, Azure Security Center, and Azure Sentinel
- Azure data retention thresholds and archiving requirements:
  - The default retention period for Azure Monitor logs is 30 days, with a maximum of two years.

- The default retention period for Azure AD reports (premium) is 30 days.
    - The default retention period for the Azure diagnostic service is 90 days.
  - Operational requirements:
    - Operational dashboards with native tools such as Azure Monitor logs or third-party tooling
    - Controlling privileged activities with centralized roles
    - [Managed identities for Azure resources](#) for access to Azure services
    - Resource locks to protect editing and deleting resources
- Design recommendations:**
- Use a single [monitor logs workspace](#) to manage platforms centrally except where role-based access control (RBAC), data sovereignty requirements and data retention policies mandate separate workspaces. Centralized logging is critical to the visibility required by operations management teams. Logging centralization drives reports about change management, service health, configuration, and most other aspects of IT operations. Converging on a centralized workspace model reduces administrative effort and the chances for gaps in observability.
- In the context of the enterprise-scale architecture, centralized logging is primarily concerned with platform operations. This emphasis doesn't prevent the use of the same workspace for VM-based application logging. With a workspace configured in resource-centric access control mode, granular RBAC is enforced to ensure app teams will only have access to the logs from their resources. In this model, app teams benefit from the use of existing platform infrastructure by reducing their management overhead. For any non-compute resources such as web apps or Azure Cosmos DB databases, application teams can use their own Log Analytics workspaces and configure diagnostics and metrics to be routed here.
- Export logs to Azure Storage if log retention requirements exceed two years. Use immutable storage with a write-once, read-many policy to make data non-erasable and non-modifiable for a user-specified interval.
  - Use Azure Policy for access control and compliance reporting. Azure Policy provides the ability to enforce organization-wide settings to ensure consistent policy adherence and fast violation detection. For more information, see [Understand Azure Policy effects](#).
  - Monitor in-guest virtual machine (VM) configuration drift using Azure Policy. Enabling [guest configuration](#) audit capabilities through policy helps app team workloads to immediately consume feature capabilities with little effort.
  - Use [update management in Azure Automation](#) as a long-term patching mechanism for both Windows and Linux VMs. Enforcing update management configurations through policy ensures that all VMs are included in the patch management regimen and provides application teams with the ability to manage patch deployment for their VMs. It also provides visibility and enforcement capabilities to the central IT team across all VMs.
  - Use Network Watcher to proactively monitor traffic flows via [Network Watcher NSG flow logs v2](#). [Traffic Analytics](#) analyzes NSG flow logs to gather deep insights about IP traffic within a virtual network and provides critical information for effective management and monitoring. Traffic Analytics provide information such as most communicating hosts and app protocols, most conversing host pairs, allowed or blocked traffic, inbound and outbound traffic, open internet ports, most blocking rules, traffic distribution per an Azure datacenter, virtual network, subnets, or rogue networks.
  - Use resource locks to prevent accidental deletion of critical shared services.
  - Use [deny policies](#) to supplement Azure AD RBAC assignments. Deny policies are used to prevent deploying and configuring resources that don't match defined standards by preventing the request from being sent to the resource provider. The combination of deny policies and RBAC assignments ensures the appropriate guardrails are in place to enforce *who* can deploy and configure resources and *what* resources they can deploy and configure.
  - Include [service](#) and [resource](#) health events as part of the overall platform monitoring solution. Tracking service and resource health from the platform perspective is an important component of resource management in

Azure.

- Don't send raw log entries back to on-premises monitoring systems. Instead, adopt a principle that *data born in Azure stays in Azure*. If on-premises SIEM integration is required, then [send critical alerts](#) instead of logs.

## Plan for app management and monitoring

To expand on the previous section, this section will consider a federated model and explain how application teams can operationally maintain these workloads.

### Design considerations:

- Application monitoring can use dedicated Log Analytics workspaces.
- For applications that are deployed to virtual machines, logs should be stored centrally to the dedicated Log Analytics workspace from a platform perspective. Application teams can access the logs subject to the RBAC they have on their applications or virtual machines.
- App performance and health monitoring for both infrastructure as a service (IaaS) and platform as a service (PaaS) resources.
- Data aggregation across all app components.
- [Health modeling and operationalization](#):
  - How to measure the health of the workload and its subsystems
  - A traffic-light model to represent health
  - How to respond to failures across app components

### Design recommendations:

- Use a centralized Azure Monitor Log Analytics workspace to collect logs and metrics from IaaS and PaaS app resources and [control log access with RBAC](#).
- Use [Azure Monitor metrics](#) for time-sensitive analysis. Metrics in Azure Monitor are stored in a time-series database optimized to analyze time-stamped data. These metrics are well suited for alerts and detecting issues quickly. They can also tell you how your system is performing. They typically need to be combined with logs to identify the root cause of issues.
- Use [Azure Monitor logs](#) for insights and reporting. Logs contain different types of data that's organized into records with different sets of properties. They're useful for analyzing complex data from a range of sources, such as performance data, events, and traces.
- When necessary, use shared storage accounts within the landing zone for Azure diagnostic extension log storage.
- Use [Azure Monitor alerts](#) for the generation of operational alerts. Azure Monitor alerts unify alerts for metrics and logs and use features such as action and smart groups for advanced management and remediation purposes.

# Enterprise-scale business continuity and disaster recovery

11/9/2020 • 2 minutes to read • [Edit Online](#)

Your organization or enterprise needs to design suitable, platform-level capabilities that application workloads can consume to meet their specific requirements. Specifically, these application workloads have requirements pertaining to recover time objective (RTO) and recovery point objective (RPO). Be sure that you capture disaster recovery (DR) requirements in order to design capabilities appropriately for these workloads.

## Design considerations

Consider the following factors:

- Application and data availability requirements, and the use of active-active and active-passive availability patterns (such as workload RTO and RPO requirements).
- Business continuity and DR for platform as a service (PaaS) services, and the availability of native DR and high-availability features.
- Support for multiregion deployments for failover purposes, with component proximity for performance reasons.
- Application operations with reduced functionality or degraded performance in the presence of an outage.
- Workload suitability for Availability Zones or availability sets.
  - Data sharing and dependencies between zones.
  - The impact of Availability Zones on update domains compared to availability sets and the percentage of workloads that can be under maintenance simultaneously.
  - Support for specific virtual machine (VM) stock-keeping units with Availability Zones.
  - Using Availability Zones is required if Microsoft Azure ultra disk storage is used.
- Consistent backups for applications and data.
  - VM snapshots and using Azure Backup and Recovery Services vaults.
  - Subscription limits restricting the number of Recovery Services vaults and the size of each vault.
  - Geo-replication and DR capabilities for PaaS services.
- Network connectivity if a failover occurs.
  - Bandwidth capacity planning for Azure ExpressRoute.
  - Traffic routing if a regional, zonal, or network outage occurs.
- Planned and unplanned failovers.
  - IP address consistency requirements and the potential need to maintain IP addresses after failover and failback.
  - Maintained engineering DevOps capabilities.
- Azure Key Vault DR for application keys, certificates, and secrets.

## Design recommendations

The following are best practices for your design:

- Employ Azure Site Recovery for Azure-to-Azure Virtual Machines disaster recovery scenarios. This enables you to replicate workloads across regions.

Site Recovery provides built-in platform capabilities for VM workloads to meet low RPO/RTO requirements through real-time replication and recovery automation. Additionally, the service provides the ability to run recovery drills without affecting the workloads in production. You can use Azure Policy to enable replication and also audit the protection of your VMs.

- Use native PaaS service disaster recovery capabilities.

The built-in features provide an easy solution to the complex task of building replication and failover into a workload architecture, simplifying both design and deployment automation. An organization that has defined a standard for the services they use can also audit and enforce the service configuration through Azure Policy.

- Use Azure-native backup capabilities.

Azure Backup and PaaS-native backup features remove the need for managing third-party backup software and infrastructure. As with other native features, you can set, audit, and enforce backup configurations with Azure Policy. This ensures that services remain compliant with the organization's requirements.

- Use multiple regions and peering locations for ExpressRoute connectivity.

A redundant hybrid network architecture can help ensure uninterrupted cross-premises connectivity in the event of an outage affecting an Azure region or peering provider location.

- Avoid using overlapping IP address ranges for production and DR sites.

When possible, plan for a business continuity and DR network architecture that provides concurrent connectivity to all sites. DR networks that use the same classless inter-domain routing blocks, such as production networks, require a network failover process that can complicate and delay application failover in the event of an outage.

# Enterprise-scale security governance and compliance

11/9/2020 • 10 minutes to read • [Edit Online](#)

This article covers defining encryption and key management, planning for governance, defining security monitoring and an audit policy, and planning for platform security. At the end of the article, you can refer to a table that describes a framework to assess enterprise security readiness of Azure services.

## Define encryption and key management

Encryption is a vital step toward ensuring data privacy, compliance, and data residency in Microsoft Azure. It's also one of the most important security concerns of many enterprises. This section covers design considerations and recommendations as they pertain to encryption and key management.

### Design considerations

- Subscription and scale limits as they apply to Azure Key Vault: Key Vault has transaction limits for keys and secrets. To throttle transactions per vault in a certain period, see [Azure limits](#).
- Key Vault serves a security boundary because access permissions for keys, secrets, and certificates are at the vault level. Key Vault access policy assignments grant permissions separately to keys, secrets, or certificates. They don't support granular, object-level permissions like a specific key, secret, or certificate [key management](#).
- You can isolate application-specific and workload-specific secrets and shared secrets, as appropriate [control access](#).
- You can optimize premium SKUs where hardware-security-module-protected keys are required. Underlying hardware security modules (HSMs) are FIPS 140-2 level 2 compliant. Manage Azure dedicated HSM for FIPS 140-2 level 3 compliance by considering the supported scenarios.
- Key rotation and secret expiration.
  - Certificate procurement and signing by using Key Vault [about certificates](#).
  - Alerting/notifications and automated certificate renewals.
- Disaster recovery requirements for keys, certificates, and secrets.

Key Vault service replication and failover capabilities: [availability and redundancy](#).

- Monitoring key, certificate, and secret usage.

Detecting unauthorized access by using a key vault or Azure Monitor Log Analytics workspace: [monitoring and alerting](#).

- Delegated Key Vault instantiation and privileged access: [secure access](#).
- Requirements for using customer-managed keys for native encryption mechanisms such as Azure Storage encryption:
  - [Customer-managed keys](#).
  - Whole-disk encryption for virtual machines (VMs).
  - Data-in-transit encryption.
  - Data-at-rest encryption.

### Design recommendations

- Use a federated Azure Key Vault model to avoid transaction scale limits.
- Provision Azure Key Vault with the soft delete and purge policies enabled to allow retention protection for deleted objects.
- Follow a least privilege model by limiting authorization to permanently delete keys, secrets, and certificates to specialized custom Azure Active Directory (Azure AD) roles.
- Automate the certificate management and renewal process with public certificate authorities to ease administration.
- Establish an automated process for key and certificate rotation.
- Enable firewall and virtual network service endpoint on the vault to control access to the key vault.
- Use the platform-central Azure Monitor Log Analytics workspace to audit key, certificate, and secret usage within each instance of Key Vault.
- Delegate Key Vault instantiation and privileged access and use Azure Policy to enforce a consistent compliant configuration.
- Default to Microsoft-managed keys for principal encryption functionality and use customer-managed keys when required.
- Don't use centralized instances of Key Vault for application keys or secrets.
- Don't share Key Vault instances between applications to avoid secret sharing across environments.

## Plan for governance

Governance provides mechanisms and processes to maintain control over your applications and resources in Azure. Azure Policy is essential to ensuring security and compliance within enterprise technical estates. It can enforce vital management and security conventions across Azure platform services and supplement role-based access control (RBAC) that controls what actions authorized users can perform.

### Design considerations

- Determine what Azure policies are needed.
- Enforce management and security conventions, such as the use of private endpoints.
- Manage and create policy assignments by using policy definitions can be reused at multiple inherited assignment scopes. You can have centralized, baseline policy assignments at management group, subscription, and resource group scopes.
- Ensure continuous compliance with compliance reporting and auditing.
- Understand that Azure Policy has limits, such as the restriction of definitions at any particular scope: [policy limits](#).
- Understand regulatory compliance policies. These might include the health insurance portability and accountability act, payment card industry, data security standards, service organization controls trust service principals, and criteria.

### Design recommendations

- Identify required Azure tags and use the append policy mode to enforce usage.
- Map regulatory and compliance requirements to Azure Policy definitions and Azure AD RBAC assignments.
- Establish Azure Policy definitions at the top-level root management group so that they can be assigned at inherited scopes.

- Manage policy assignments at the highest appropriate level with exclusions at bottom levels, if required.
- Use Azure Policy to control resource provider registrations at the subscription and/or management group levels.
- Use built-in policies where possible to minimize operational overhead.
- Assign the built-in policy contributor role at a particular scope to enable application-level governance.
- Limit the number of Azure Policy assignments made at the root management group scope to avoid managing through exclusions at inherited scopes.

## Define security monitoring and an audit policy

An enterprise must have visibility into what's happening within their technical cloud estate. Security monitoring and audit logging of Azure platform services is a key component of a scalable framework.

### **Design considerations**

- Data retention periods for audit data. Azure AD Premium reports have a 30-day retention period.
- Long-term archiving of logs such as Azure activity logs, VM logs, and platform as a service (PaaS) logs.
- Baseline security configuration via Azure in-guest VM policy.
- Emergency patching for critical vulnerabilities.
- Patching for VMs that are offline for extended periods of time.
- Requirements for real-time monitoring and alerting.
- Security information and event management integration with Azure Security Center and Azure Sentinel.
- Vulnerability assessment of VMs.

### **Design recommendations**

- Use Azure AD reporting capabilities to generate access control audit reports.
- Export Azure activity logs to Azure Monitor logs for long-term data retention. Export to Azure Storage for long-term storage beyond two years, if necessary.
- Enable Security Center Standard for all subscriptions, and use Azure Policy to ensure compliance.
- Monitor base operating system patching drift via Azure Monitor logs and Azure Security Center.
- Use Azure policies to automatically deploy software configurations through VM extensions and enforce a compliant baseline VM configuration.
- Monitor VM security configuration drift via Azure Policy.
- Connect default resource configurations to a centralized Azure Monitor Log Analytics workspace.
- Use an Azure Event Grid-based solution for log-oriented, real-time alerting.

## Plan for platform security

You must maintain a healthy security posture as you adopt Azure. Besides visibility, you have to be able to control the initial settings and changes as the Azure services evolve. Therefore, planning for platform security is key.

### **Design considerations**

- Shared responsibility.

- High availability and disaster recovery.
- Consistent security across Azure services in terms of data management and control plane operations.
- Multitenancy for key platform components. This includes Hyper-V, the HSMs underpinning Key Vault, and database engines.

### Design recommendations

- In the context of your underlying requirements, conduct a joint examination of each required service. If you want to bring your own keys, this might not be supported across all considered services. Implement relevant mitigation so that inconsistencies don't hinder desired outcomes. Choose appropriate region pairs and disaster recovery regions that minimize latency.
- Develop a security allow-list plan to assess services security configuration, monitoring, alerts, and how to integrate these with existing systems.
- Determine the incident response plan for Azure services before allowing it into production.
- Use Azure AD reporting capabilities to generate access control audit reports.
- Align your security requirements with Azure platform roadmaps to stay current with newly released security controls.
- Implement a zero-trust approach for access to the Azure platform, where appropriate.

## Azure Security Benchmarks

The Azure Security Benchmark includes a collection of high-impact security recommendations you can use to help secure most of the services you use in Azure. You can think of these recommendations as "general" or "organizational" as they are applicable to most Azure services. The Azure Security Benchmark recommendations are then customized for each Azure service, and this customized guidance is contained in service recommendations articles.

The Azure Security Benchmark documentation specifies security controls and service recommendations.

- [Security Controls](#): The Azure Security Benchmark recommendations are categorized by security controls. Security controls represent high-level vendor-agnostic security requirements, such as network security and data protection. Each security control has a set of security recommendations and instructions that help you implement those recommendations.
- [Service Recommendations](#): When available, benchmark recommendations for Azure services will include Azure Security Benchmark recommendations that are tailored specifically for that service.

## Service enablement framework

As business units request to deploy workloads to Azure, you need additional visibility into a workload to determine how to achieve appropriate levels of governance, security, and compliance. When a new service is required, you need to allow it. The following table provides a framework to assess enterprise security readiness of Azure services:

ASSESSMENT	CATEGORY	CRITERIA
Security	Network endpoint	Does the service have a public endpoint that is accessible outside of a virtual network?
		Does it support virtual network service endpoints?

ASSESSMENT	CATEGORY	CRITERIA
		Can Azure services interact directly with the service endpoint?
		Does it support Azure Private Link endpoints?
		Can it be deployed within a virtual network?
	Data exfiltration prevention	Does the PaaS service have a separate border gateway protocol community in Azure ExpressRoute Microsoft peering? Does ExpressRoute expose a route filter for the service?
		Does the service support Private Link endpoints?
	Enforce network traffic flow for management and data plane operations	Is it possible to inspect traffic entering/exiting the service? Can traffic be force-tunneled with user-defined routing?
		Do management operations use Azure shared public IP ranges?
		Is management traffic directed via a link-local endpoint exposed on the host?
	Data encryption at-rest	Is encryption applied by default?
		Can encryption be disabled?
		Is encryption performed with Microsoft-managed keys or customer-managed keys?
	Data encryption in-transit	Is traffic to the service encrypted at a protocol level (secure sockets layer/transport layer security)?
		Are there any HTTP endpoints, and can they be disabled?
		Is underlying service communication also encrypted?
		Is encryption performed with Microsoft-managed keys or customer-managed keys? (Is bring your own encryption supported?)
	Software deployment	Can application software or third-party products be deployed to the service?

ASSESSMENT	CATEGORY	CRITERIA
		How is software deployment performed and managed?
		Can policies be enforced to control source or code integrity?
		If software is deployable, can antimalware capability, vulnerability management, and security monitoring tools be used?
		Does the service provide such capabilities natively, such as with Azure Kubernetes Service?
Identity and access management	Authentication and access control	Are all control plane operations governed by Azure AD? Is there a nested control plane, such as with Azure Kubernetes Service?
		What methods exist to provide access to the data plane?
		Does the data plane integrate with Azure AD?
		Does Azure-to-Azure (service-to-service) authentication use an MSI/service principal?
		Is Azure-to-IaaS (service-to-virtual-network) authentication via Azure AD?
		How are any applicable keys or shared access signatures managed?
		How can access be revoked?
	Segregation of duties	Does the service separate control plane and data plane operations within Azure AD?
	Multi-factor authentication and conditional access	Is multi-factor authentication enforced for user to service interactions?
Governance	Data export and import	Does service allow you to import and export data securely and encrypted?
	Data privacy and usage	Can Microsoft engineers access the data?

ASSESSMENT	CATEGORY	CRITERIA
		Is any Microsoft Support interaction with the service audited?
	Data residency	Is data contained to the service deployment region?
Operations	Monitoring	Does the service integrate with Azure Monitor?
	Backup management	Which workload data need to be backed up?
		How are backups captured?
		How frequently can backups be taken?
		How long can backups be retained for?
		Are backups encrypted?
		Is backup encryption performed with Microsoft-managed keys or customer-managed keys?
	Disaster recovery	How can the service be used in a regional redundant fashion?
		What is the attainable recovery time objective and recovery point objective?
	SKU	What SKUs are available? And how do they differ?
		Are there any features related to security for Premium SKU?
	Capacity management	How is capacity monitored?
		What is the unit of horizontal scale?
	Patch and update management	Does the service require active updating or do updates happen automatically?
		How frequently are updates applied? Can they be automated?
	Audit	Are nested control plane operations captured (for example, Azure Kubernetes Service or Azure Databricks)?
		Are key data plane activities recorded?

ASSESSMENT	CATEGORY	CRITERIA
	Configuration management	Does it support tags and provide a <code>put</code> schema for all resources?
Azure service compliance	Service attestation, certification, and external audits	Is the service PCI/ISO/SOC compliant?
	Service availability	Is the service a private preview, a public preview, or generally available?
		In what regions is the service available?
		What is the deployment scope of the service? Is it a regional or global service?
	Service-level agreements (SLAs)	What is the SLA for service availability?
		If applicable, what is the SLA for performance?

# Platform automation and DevOps

11/9/2020 • 4 minutes to read • [Edit Online](#)

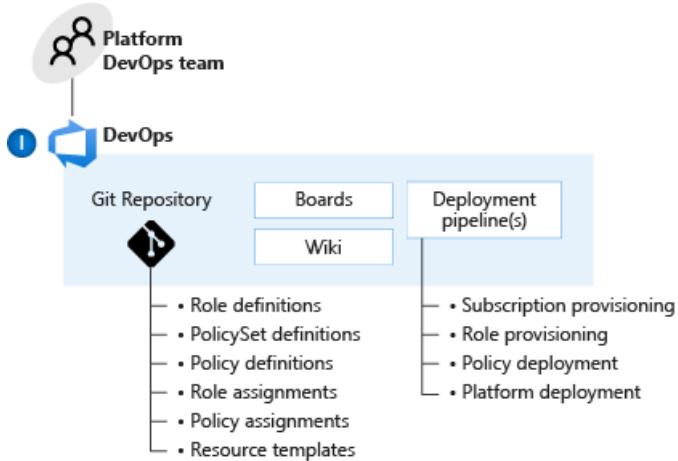


Figure 1: Platform automation and DevOps.

## Planning for a DevOps approach

Many traditional IT operating models aren't compatible with the cloud, and organizations must undergo operational and organizational transformation to deliver against enterprise migration targets. You should use a DevOps approach for both application and central teams.

### Design considerations

- Where central teams are concerned, you should use pipelines for continuous integration and continuous deployment. Use the pipelines to manage policy definitions, role definitions, policy assignments, management group hierarchies, and subscriptions. These pipelines help ensure that you can operationally manage multiple subscriptions while still conforming to a desired state.
- The blanket application of a DevOps model won't instantly establish capable DevOps teams.
- Investing in engineering capabilities and resources is critical.
- You can arrange internal and external DevOps roles and functions from a variety of sources that align with your organization's strategy.
- For some legacy apps, the associated app team might not have engineering resources required to align with a DevOps strategy.

### Design recommendations

Establish a cross-functional DevOps platform team to build, manage, and maintain your enterprise-scale architecture. This team should include members from your central IT team, security, compliance, and business units to ensure that a wide spectrum of your enterprise is represented. The following list presents a recommended set of DevOps roles for a central platform team:

- **PlatformOps** (platform operations) for:
  - Subscription provisioning and delegation of required network, identity and access management, and policies.
  - Platform management and monitoring (holistic).

- Cost management (holistic).
  - Platform-as-code (managing templates, scripts, and other assets).
  - Responsible for overall operations on Microsoft Azure within the Azure Active Directory tenant (managing service principals, Graph API registration, and defining roles).
- **SecOps** (security operations)
  - Role-based access control (RBAC) (holistic).
  - Key management (for central services, simple mail-transfer protocol, and domain controller).
  - Policy management and enforcement (holistic).
  - Security monitoring and audit (holistic).
- **NetOps** (network operations)
  - Network management (holistic).
- **AppDevOps**. Allow app owners to create and manage app resources through a DevOps model. The following list presents a recommended DevOps role for application teams:
  - App migration or transformation.
  - App management and monitoring.
  - RBAC (app resources).
  - Security monitoring and audit (app resources).
  - Cost management (app resources).
  - Network management (app resources).
  - In some instances, you might want to break AppDevOps into more granular roles such as AppDataOps for database management or AppSecOps for more security-sensitive apps.
  - Provide a central app DevOps function to support apps that don't have existing DevOps capabilities or a business case to establish one (for example, legacy apps with minimal development capabilities).
  - Use a policy-driven approach with clear RBAC boundaries to centrally enforce consistency and security across application teams. This ensures a least privilege approach is taken by using a combination of RBAC assignments and Azure Policy, and that workloads are compliant with Azure Policy assignments at all times.
  - To accelerate Azure adoption, the central platform team should establish a common set of templates and libraries for application teams to draw upon. For example, horizontal (cross-function) guidance can help to support migrations through subject matter expertise and to ensure alignment with the overall target enterprise-scale architecture.
  - Don't restrict application teams to use central artifacts or approaches because it hinders their agility. You can enforce consistent baseline configurations through a policy-driven infrastructure approach and RBAC assignments. This ensures that app (business unit) teams are flexible enough to innovate while still able to draw from a predefined set of templates.
  - Don't force application teams to use a central process or provisioning pipeline for the instantiation or management of app resources. Existing teams that already rely on a DevOps pipeline for app delivery should still be able to use the same tools they have been using. Remember that you can still use Azure Policy to maintain guard rails, independent of how resources are deployed in Azure.

# Define central and federated responsibilities

The distribution of roles, responsibilities, and trust between central IT teams and apps teams is paramount to the operational transformation your organization must undergo when adopting the cloud at scale.

## Design considerations

Central teams strive to maintain full control while app owners seek to maximize agility. The balance between these goals can greatly influence the success of the migration.

## Design recommendations

The following list presents a recommended distribution of responsibilities between the central IT team and application teams. You're striving to empower migration and transformation activities with minimal central dependencies. At the same time, you want to support the centralized governance of security and operability across the entire estate.

- **App functions**

- App migration and transformation.
- App management and monitoring (app resources).
- Key management (app keys).
- RBAC (app resources).
- Security monitoring and audit (app resources).
- Cost management (app resources).
- Network management (app resources).

- **Central functions**

- Architecture governance.
- Subscription management.
- Platform as code (management of templates, scripts, and other assets).
- Policy management and enforcement (holistic).
- Platform management and monitoring (holistic).
- RBAC (holistic).
- Key management (central services).
- Network management (including networks and network virtual appliances).
- Security monitoring and audit (holistic).
- Cost management (holistic).

An Azure DevOps model that's based on these recommendations provides the desired control for central teams and the migration agility required by application teams.

# Enterprise-scale implementation guidelines

11/9/2020 • 8 minutes to read [Edit Online](#)

This article covers how to get started with the enterprise-scale, platform-native reference implementation and outline design objectives.

In order to implement the enterprise-scale architecture, you must think in terms of the following categories of activities:

1. **What must be true for the enterprise-scale architecture:** Encompasses activities that must be performed by the Azure and Azure Active Directory (Azure AD) administrators to establish an initial configuration. These activities are sequential by nature and primarily one-off activities.
2. **Enable a new region (File > New > Region):** Encompasses activities that are required whenever there is a need to expand the enterprise-scale platform into a new Azure region.
3. **Deploy a new landing zone (File > New > Landing Zone):** These are recurring activities that are required to instantiate a new landing zone.

To operationalize at scale, these activities must follow infrastructure-as-code (IaC) principles and must be automated by using deployment pipelines.

## What must be true for an enterprise-scale landing zone

The following sections list the steps to complete this category of activity in the Microsoft Cloud Adoption Framework for Azure.

### Enterprise Agreement enrollment and Azure AD tenants

1. Set up the Enterprise Agreement (EA) administrator and notification account.
2. Create departments: business domains/geo-based/org.
3. Create an EA account under a department.
4. Set up Azure AD Connect for each Azure AD tenant if the identity is to be synchronized from on-premises.
5. Establish zero standing access to Azure resources and just-in-time access via Azure AD Privileged Identity Management (PIM).

### Management group and subscription

1. Create a management group hierarchy by following the recommendations in [Management group and subscription organization](#).
2. Define the criteria for subscription provisioning and the responsibilities of a subscription owner.
3. Create management, connectivity, and identity subscriptions for platform management, global networking, and connectivity and identity resources like Active Directory domain controllers.
4. Set up a Git repository to host IaC and service principals for use with a platform pipeline for continuous integration and continuous deployment.
5. Create custom role definitions and manage entitlements by using Azure AD PIM for subscription and management group scopes.
6. Create the Azure Policy assignments in the following table for the landing zones.

NAME	DESCRIPTION
Deny-PublicEndpoints	Denies the creation of services with public endpoints on all landing zones.
Deploy-VM-Backup	Ensures that backup is configured and deployed to all VMs in the landing zones.
Deploy-VNet	Ensures that all landing zones have a virtual network deployed and that it's peered to the regional virtual hub.

#### Sandbox Governance Guidance

As detailed in the [Management group and subscription organization critical design area](#), subscriptions placed within the Sandbox Management Group hierarchy should have a less restrictive policy approach. As these subscriptions should be used by users within the business to experiment and innovate with Azure products and services, that may not be yet permitted in your Landing Zones hierarchy, to validate if their ideas/concepts could work; before they move into a formal development environment.

However these subscriptions in the Sandbox Management Group hierarchy do still require some guardrails applied to ensure they are only used in the correct manner; e.g. for innovation, trialling new Azure services/products/features and ideation validation.

#### We therefore recommend:

1. Create the Azure Policy assignments in the following table at the Sandbox Management Group scope:

NAME	DESCRIPTION	ASSIGNMENT NOTES
Deny-VNET-Peering-Cross-Subscription	Prevents VNET peering connections being created to other VNETs outside of the subscription.	Ensure this policy is only assigned to the Sandbox Management Group hierarchy scoping level.
Denied-Resources	Resources that are denied from creation in the sandbox subscriptions. This will prevent any hybrid connectivity resources from being created; e.g. <i>VPN/ExpressRoute/VirtualWAN</i>	When assigning this policy select the following resources to deny the creation of: VPN Gateways: <code>microsoft.network/vpngateways</code> , P2S Gateways: <code>microsoft.network/p2svpngateways</code> , Virtual WANs: <code>microsoft.network/virtualwans</code> , Virtual WAN Hubs: <code>microsoft.network/virtualhubs</code> , ExpressRoute Circuits: <code>microsoft.network/expressrouteconnections</code> , ExpressRoute Gateways: <code>microsoft.network/expressroutegateways</code> , ExpressRoute Ports: <code>microsoft.network/expressrouteports</code> , ExpressRoute Cross-Connections: <code>microsoft.network/expressrouteconnections</code> and Local Network Gateways: <code>microsoft.network/localnetworkgateways</code> .

NAME	DESCRIPTION	ASSIGNMENT NOTES
<a href="#">Deploy-Budget-Sandbox</a>	Ensures a budget exists for each sandbox subscription, with e-mail alerts enabled. The budget will be named: <code>default-sandbox-budget</code> in each subscription.	If during the assignment of the policy the parameters are not amended from their defaults a the budget ( <code>default-sandbox-budget</code> ) will be created with a 1000 currency threshold limit and will send an e-mail alert to the subscription's owners and contributors (based on RBAC role assignment) at 90% and 100% of the budget threshold.

## Global networking and connectivity

1. Allocate an appropriate virtual network CIDR range for each Azure region where virtual hubs and virtual networks will be deployed.
2. If you decide to create the networking resources via Azure Policy, assign the policies listed in the following table to the connectivity subscription. By doing this, Azure Policy ensures the resources in the following list are created based on parameters provided.
  - Create an Azure Virtual WAN Standard instance.
  - Create an Azure Virtual WAN virtual hub for each region. Ensure that at least one gateway (Azure ExpressRoute or VPN) per virtual hub is deployed.
  - Secure virtual hubs by deploying Azure Firewall within each virtual hub.
  - Create required Azure Firewall policies and assign them to secure virtual hubs.
  - Ensure that all virtual networks connected to a secure virtual hub are protected by Azure Firewall.
3. Deploy and configure an Azure Private DNS zone.
4. Provision ExpressRoute circuits with Azure private peering. Follow the instructions in [Create and modify peering for an ExpressRoute circuit](#).
5. Connect on-premises HQs/DCs to Azure Virtual WAN virtual hubs via ExpressRoute circuits.
6. Protect virtual network traffic across virtual hubs with network security groups (NSGs).
7. (Optional) Set up encryption over ExpressRoute private peering. Follow the instructions in [ExpressRoute encryption: IPsec over ExpressRoute for Virtual WAN](#).
8. (Optional) Connect branches to the virtual hub via VPN. Follow the instructions in [Create a Site-to-Site connection using Azure Virtual WAN](#).
9. (Optional) Configure ExpressRoute Global Reach for connecting on-premises HQs/DCs when more than one on-premises location is connected to Azure via ExpressRoute. Follow the instructions in [Configure ExpressRoute Global Reach](#).

The following list shows Azure Policy assignments that you use when you're implementing networking resources for an enterprise-scale deployment:

NAME	DESCRIPTION
<a href="#">Deploy-FirewallPolicy</a>	Creates a firewall policy.
<a href="#">Deploy-VHub</a>	This policy deploys a virtual hub, Azure Firewall, and VPN/ExpressRoute gateways. It also configures the default route on connected virtual networks to Azure Firewall.
<a href="#">Deploy-VWAN</a>	Deploys a Virtual WAN.

## Security, governance, and compliance

1. Define and apply a [service enablement framework](#) to ensure Azure services meet enterprise security and governance requirements.
2. Create custom role-based access control definitions.
3. Enable Azure AD PIM and discover Azure resources to facilitate PIM.
4. Create Azure AD-only groups for the Azure control plane management of resources by using Azure AD PIM.
5. Apply policies listed in the following table to ensure Azure services are compliant to enterprise requirements.
6. Define a naming convention and enforce it via Azure Policy.
7. Create a policy matrix at all scopes (for example, enable monitoring for all Azure services via Azure Policy).

The following policies should be used to enforce company-wide compliance status.

NAME	DESCRIPTION
<a href="#">Allowed-ResourceLocation</a>	Specifies the allowed region where resources can be deployed.
<a href="#">Allowed-RGLocation</a>	Specifies the allowed region where resource groups can be deployed.
<a href="#">Denied-Resources</a>	Resources that are denied for the company.
<a href="#">Deny-AppGW-Without-WAF</a>	Allows application gateways deployed with Azure Web Application Firewall enabled.
<a href="#">Deny-IP-Forwarding</a>	Denies IP forwarding.
<a href="#">Deny-RDP-From-Internet</a>	Denies RDP connections from the internet.
<a href="#">Deny-Subnet-Without-Nsg</a>	Denies subnet creation without an NSG.
<a href="#">Deploy-ASC-CE</a>	Sets up Azure Security Center continuous export to your Log Analytics workspace.
<a href="#">Deploy-ASC-Monitoring</a>	Enables monitoring in Security Center.
<a href="#">Deploy-ASC-Standard</a>	Ensures that subscriptions have Security Center Standard enabled.
<a href="#">Deploy-Diag-ActivityLog</a>	Enables diagnostics activity log and forwarding to Log Analytics.
<a href="#">Deploy-Diag-LogAnalytics</a>	
<a href="#">Deploy-VM-Monitoring</a>	Ensures that VM monitoring is enabled.

## Platform identity

1. If you create the identity resources via Azure Policy, assign the policies listed in the following table to the identity subscription. By doing this, Azure Policy ensures that the resources in the following list are created based on the parameters provided.
2. Deploy the Active Directory domain controllers.

The following list shows policies that you can use when you're implementing identity resources for an enterprise-scale deployment.

NAME	DESCRIPTION
DataProtectionSecurityCenter	Data protection automatically created by Security Center.
Deploy-VNet-Identity	Deploys a virtual network into the identity subscription to host (for example, DC).

## Platform management and monitoring

1. Create policy compliance and security dashboards for organizational and resource-centric views.
2. Create a workflow for platform secrets (service principals and automation account) and key rollover.
3. Set up long-term archiving and retention for logs within Log Analytics.
4. Set up Azure Key Vault to store platform secrets.
5. If you create the platform management resources via Azure Policy, assign the policies listed in the following table to the management subscription. By doing this, Azure Policy ensures that the resources in the following list are created based on parameters provided.

NAME	DESCRIPTION
Deploy-LA-Config	Configuration of the Log Analytics workspace.
Deploy-Log-Analytics	Deploys a Log Analytics workspace.

## File > New > Region

1. If you create the networking resources via Azure Policy, assign the policies listed in the following table to the connectivity subscription. By doing this, Azure Policy ensures that the resources in the following list are created based on parameters provided.
  - In the connectivity subscription, create a new virtual hub within the existing Virtual WAN.
  - Secure virtual hub by deploying Azure Firewall within the virtual hub and link existing or new firewall policies to Azure Firewall.
  - Ensure that all virtual networks connected to a secure virtual hub are protected by Azure Firewall.
2. Connect the virtual hub to the on-premises network via either ExpressRoute or VPN.
3. Protect virtual network traffic across virtual hubs via NSGs.
4. (Optional) Set up encryption over ExpressRoute private peering.

NAME	DESCRIPTION
Deploy-VHub	This policy deploys a virtual hub, Azure Firewall, and gateways (VPN/ExpressRoute). It also configures the default route on connected virtual networks to Azure Firewall.

## File > New > Landing Zone for applications and workloads

1. Create a subscription and move it under the `Landing Zones` management group scope.
2. Create Azure AD groups for the subscription, such as `Owner`, `Reader`, and `Contributor`.
3. Create Azure AD PIM entitlements for established Azure AD groups.

# Transition existing Azure environments to Enterprise-Scale

11/9/2020 • 4 minutes to read • [Edit Online](#)

We recognize that most organizations may have an existing footprint in Azure, one or more subscriptions, and potentially an existing structure of their management groups. Depending on their initial business requirements and scenarios, Azure resources such as hybrid connectivity (for example with Site-to-Site VPN and/or ExpressRoute) may have been deployed.

This article helps organizations to navigate the right path based on an existing Azure environment transitioning into Enterprise-Scale. This article also describes considerations for moving resources in Azure (for example, moving a subscription from one existing management group to another management group), which will help you evaluate and plan for transitioning your existing Azure environment to Enterprise-Scale landing zones.

## Moving resources in Azure

Some resources in Azure can be moved post creation, and there are different approaches organizations can take subject to users RBAC permissions at – and across scopes. The following table outlines which resources can be moved, at which scope, and the pros/cons associated with each.

SCOPE	DESTINATION	PROS	CONS
Resources in resource groups	Can be moved to new resource group in same or different subscription	Allows you to modify resource composition in a resource group after deployment	- Not supported by all resourceTypes - Some resourceTypes have specific limitations or requirements - Resourcelds are updated and impacts existing monitoring, alerts, and control plane operations - Resource groups are locked during the move period - Requires assessment of policies and RBAC pre and post-move operation
Subscriptions in a tenant	Can be moved to different management groups, and different tenants	No impact to existing resources within the subscription, as no resourceld's will be changed	Requires assessment of policies and RBAC pre and post-move operation

To understand which move strategy you should use, we will go through examples of both:

## Subscription move

The common use cases for moving subscriptions are to organize subscriptions into management groups or when transferring subscriptions to a new Azure Active Directory tenant. Subscription moves for enterprise-scale focuses on moving subscriptions to management groups. Moving a subscription to a new tenant is mainly for [transferring billing ownership](#).

### RBAC requirements

To assess a subscription prior to a move, it is important that the user has the appropriate RBAC such as being an Owner on the subscription (direct roleAssignment), and has write permission on the target management group (built-in roles that support this is Owner, Contributor, Management Group Contributor).

If the user has an inherited Owner permission on the subscription from an existing management group, the subscription can only be moved to the management group where the user has been assigned the Owner role.

## Policy

Existing subscriptions may be subject to Azure policies assigned either directly, or at the management group where they are currently located. It is important to assess current policies, and the policies that may exist in the new management group/management group hierarchy.

Azure Resource Graph can be used to perform an inventory of existing resources and compare their configuration with the policies existing at the destination.

Once subscriptions are moved to a management group with existing RBAC and policies in place, consider the following options:

- Any RBAC that is inherited to the moved subscriptions can take up to 30 minutes before the user tokens in the management group cache are refreshed. To expedite this process, you can refresh the token by signing out and in or request a new token.
- Any policy where the assignment scope includes the moved subscriptions, will perform audit operations only on the existing resources. More specifically:
  - Any existing resource in the subscription subject to **deployIfNotExists** policy effect will appear as non-compliant and will not be remediated automatically but requires user interaction to perform the remediation manually.
  - Any existing resource in the subscription subject to **deny** policy effect will appear as non-compliant and will not be rejected. User must manually mitigate this result as appropriate.
  - Any existing resource in the subscription subject to **append** and **modify** policy effect will appear as non-compliant and requires user interaction to mitigate.
  - Any existing resource in the subscription subject to **audit** and **auditIfNotExist** will appear as non-compliant and requires user interaction to mitigate.
- All new writes to resources in the moved subscription will be subject to the assigned policies at real-time as normal.

## Resource move

The primary use cases to perform a resource move is when you want to consolidate resources into the same resource group if they share the same life-cycle, or move resources to a different subscription due to cost, ownership, or RBAC requirements.

When performing a resource move, both the source resource group and the target resource group are locked (this lock will not affect any of the resources in the resource group) during the move operation, meaning you cannot add, update, or delete resources in the resource groups. A resource move operation will not change the location of the resources.

### Before you move resources

Prior to a move operation, you must verify that the [resources in scope are supported](#) as well as assessing their requirements and dependencies. For instance, moving a peered virtual network requires you to disable virtual network peering first, and re-enable the peering once the move operation has completed. This disable/re-enable dependency requires planning upfront to understand the impact to any existing workload that may be connected to your virtual networks.

### Post-move operation

When the resources are moved into a new resource group in the same subscription, any inherited RBAC and policies from management group or/and subscription scope will still apply. If you move to a resource group in a new subscription – where the subscription may be subject to other RBAC and policy assignment, same guidance applies as to the move subscription scenario to validate the resource compliance and access controls.

# Deploy a migration landing zone in Azure

11/9/2020 • 5 minutes to read • [Edit Online](#)

A migration landing zone is an environment that has been provisioned and prepared to host workloads that are being migrated from an on-premises environment into Azure.

## Deploy the blueprint

Before you use the CAF Migration landing zone blueprint in the Cloud Adoption Framework, review the following design principles, assumptions, decisions, and implementation guidance. If this guidance aligns with the desired cloud adoption plan, the [CAF Migration landing zone blueprint](#) can be deployed using the deployment steps.

### [Deploy the blueprint sample](#)

## Design principles

This implementation option provides an opinionated approach to the common design areas shared by all Azure landing zones. See the assumptions and decisions below for addition technical detail.

### **Deployment options**

This implementation option deploys a minimum viable product (MVP) to start a migration. As the migration progresses, the customer will follow a modular refactoring-based approach to mature the operating model in parallel guidance, using the [Govern methodology](#) and the [Manage methodology](#) to address those complex topics in parallel to the initial migration effort.

The specific resources deployed by this MVP approach are outlined in the [decisions](#) section below.

### **Enterprise enrollment**

This implementation option doesn't take an inherent position on enterprise enrollment. This approach is designed to be applicable to customers regardless of contractual agreements with Microsoft or Microsoft partners. Prior to deployment of this implementation option, it is assumed that the customer has created a target subscription.

### **Identity**

This implementation option assumes that the target subscription is already associated with an Azure Active Directory instance in accordance with [identity management best practices](#)

### **Network topology and connectivity**

This implementation option creates a virtual network with subnets for gateway, firewall, jump box, and landing zone. As a next step iteration, the team would follow the [networking decisions guide](#) to implement the appropriate form of connectivity between the gateway subnet and other networks in alignment with [network security best practices](#).

### **Resource organization**

This implementation option creates a single landing zone, in which resources will be organized into workloads defined by specific resource groups. Choosing this minimalist approach to resource organization defers the technical decision of resource organization until the team's cloud operating model is more clearly defined.

This approach is based on an assumption that the cloud adoption effort will not exceed [subscription limits](#). This option also assumes limited architectural complexity and security requirements within this landing zone.

If this changes through the course of the cloud adoption plan, the resource organization may need to be refactored using the guidance in the [Govern methodology](#).

## Governance disciplines

This implementation option doesn't implement any governance tooling. In the absence of defined policy automation, this landing zone should not be used for any mission critical workloads or sensitive data. It is assumed that this landing zone is being used for limited production deployment to initiate learning, iteration, and development of the overall operating model in parallel to these early stage migration efforts.

To accelerate parallel development of governance disciplines, review the [Govern methodology](#) and consider deploying the [CAF Foundation blueprint](#) in addition to the CAF Migration landing zone blueprint.

### WARNING

As the governance disciplines mature, refactoring may be required. Specifically, resources may later need to be [moved to a new subscription or resource group](#).

## Operations baseline

This implementation option doesn't implement any operations. In the absence of a defined operations baseline, this landing zone should not be used for any mission critical workloads or sensitive data. It is assumed that this landing zone is being used for limited production deployment to initiate learning, iteration, and development of the overall operating model in parallel to these early stage migration efforts.

To accelerate parallel development of an operations baseline, review the [Manage methodology](#) and consider deploying the [Azure server management guide](#).

### WARNING

As the operations baseline is developed, refactoring may be required. Specifically, resources may later need to be [moved to a new subscription or resource group](#).

## Business continuity and disaster recovery (BCDR)

This implementation option doesn't implement any BCDR solution. It is assumed that the solution for protection and recover will be addressed by the development of the operations baseline.

## Assumptions

This initial landing zone includes the following assumptions or constraints. If these assumptions align with your constraints, you can use the blueprint to create your first landing zone. The blueprint also can be extended to create a landing zone blueprint that meets your unique constraints.

- **Subscription limits:** This adoption effort isn't expected to exceed [subscription limits](#).
- **Compliance:** No third-party compliance requirements are needed in this landing zone.
- **Architectural complexity:** Architectural complexity doesn't require additional production subscriptions.
- **Shared services:** No existing shared services in Azure require this subscription to be treated like a spoke in a hub and spoke architecture.
- **Limited production scope:** This landing zone could potentially host production workloads. It is not a suitable environment for sensitive data or mission-critical workloads.

If these assumptions align with your current adoption needs, then this blueprint might be a starting point for building your landing zone.

## Decisions

The following decisions are represented in the landing zone blueprint.

COMPONENT	DECISIONS	ALTERNATIVE APPROACHES
Migration tools	Azure Site Recovery will be deployed and an Azure Migrate project will be created.	<a href="#">Migration tools decision guide</a>
Logging and monitoring	Operational insights workspace and diagnostic storage account will be provisioned.	
Network	A virtual network will be created with subnets for gateway, firewall, jump box, and landing zone.	<a href="#">Networking decisions</a>
Identity	It's assumed that the subscription is already associated with an Azure Active Directory instance.	<a href="#">Identity management best practices</a>
Policy	This blueprint currently assumes that no Azure policies are to be applied.	
Subscription design	N/A - designed for a single production subscription.	<a href="#">Create initial subscriptions</a>
Resource groups	N/A - designed for a single production subscription.	<a href="#">Scale subscriptions</a>
Management groups	N/A - designed for a single production subscription.	<a href="#">Organize and manage subscriptions</a>
Data	N/A	<a href="#">Choose the correct SQL Server option in Azure</a> and <a href="#">Azure data store guidance</a>
Storage	N/A	<a href="#">Azure Storage guidance</a>
Naming and tagging standards	N/A	<a href="#">Naming and tagging best practices</a>
Cost management	N/A	<a href="#">Tracking costs</a>
Compute	N/A	<a href="#">Compute options</a>

## Customize or deploy a landing zone

Learn more and download a reference sample of the CAF Migration landing zone blueprint for deployment or customization from the Azure blueprint samples.

### [Deploy the blueprint sample](#)

For guidance on customizations that should be made to this blueprint or the resulting landing zone, see the [landing zone considerations](#).

## Next steps

After deploying your first landing zone, you're ready to expand your landing zone.

### [Expand your landing zone](#)



# Deploy a CAF Foundation blueprint in Azure

11/9/2020 • 4 minutes to read • [Edit Online](#)

The CAF Foundation blueprint does not deploy a landing zone. Instead, it deploys the tools required to establish a governance MVP (minimum viable product) to begin developing your governance disciplines. This blueprint is designed to be additive to an existing landing zone and can be applied to the CAF Migration landing zone blueprint with a single action.

## Deploy the blueprint

Before you use the CAF Foundation blueprint in the Cloud Adoption Framework, review the following design principles, assumptions, decisions, and implementation guidance. If this guidance aligns with the desired cloud adoption plan, the [CAF Foundation blueprint](#) can be deployed using the deployment steps.

### [Deploy the blueprint sample](#)

## Design principles

This implementation option provides an opinionated approach to the common design areas shared by all Azure landing zones. See the assumptions and decisions below for addition technical detail.

### Deployment options

This implementation option deploys an MVP to serve as the foundation for your governance disciplines. The team will follow a modular refactoring-based approach to mature the governance disciplines using the [Govern methodology](#).

### Enterprise enrollment

This implementation option does not take an inherent position on enterprise enrollment. This approach is designed to be applicable to customers regardless of contractual agreements with Microsoft or Microsoft partners. Prior to deployment of this implementation option, it's assumed that the customer has already created a target subscription.

### Identity

This implementation option assumes that the target subscription is already associated with an Azure Active Directory instance in accordance with [identity management best practices](#).

### Network topology and connectivity

This implementation option assumes the landing zone already has a defined network topology in accordance with [network security best practices](#).

### Resource organization

This implementation option demonstrates how Azure Policy can add some elements of resource organization through the application of tags. Specifically, a `costCenter` tag will be appended to resources using Azure Policy.

The governance team should compare and contrast the elements of resource organization to be addressed by tagging versus those that should be addressed through subscription design. These fundamental decisions will inform resource organization as your cloud adoption plans progress.

To aid in this comparison early in adoption cycles, the following articles should be considered:

- [Initial Azure subscriptions](#): At this stage of adoption scale, does your operating model require two, three, or four subscriptions?

- **Scale subscriptions:** As adoption scales, what criteria will be used to drive subscription scaling?
- **Organize subscriptions:** How will you organize subscriptions as you scale?
- **Tagging standards:** What other criteria need to be consistently captured in tags to augment your subscription design?

To aid in this comparison when teams are further along with cloud adoption, see the governance patterns section of the [governance guide - prescriptive guidance](#) article. This section of the prescriptive guidance demonstrates a set of patterns based on a specific narrative and operating model. That guidance also includes links to other patterns that should be considered.

## Governance disciplines

This implementation demonstrates one approach to maturity in the Cost Management discipline of the Govern methodology. Specifically, it demonstrates how Azure Policy can be used to create an allow list of specific SKUs. Limiting the types and sizes of resources that can be deployed into a landing zone reduces the risk of overspending.

To accelerate parallel development of the other governance disciplines, review the [Govern methodology](#). To continue maturing the Cost Management discipline of governance, see the [Cost Management discipline guidance](#).

### WARNING

As the governance disciplines mature, refactoring may be required. Refactoring may be required. Specifically, resources may later need to be [moved to a new subscription or resource group](#).

## Operations baseline

This implementation option does not implement any aspects of the operations baseline. In the absence of a defined operations baseline, this landing zone should not be used for any mission critical workloads or sensitive data. It is assumed that this landing zone is being used for limited production deployment to initiate learning, iteration, and development of the overall operating model in parallel to these early stage migration efforts.

To accelerate parallel development of an operations baseline, review the [Manage methodology](#) and consider deploying the [Azure server management guide](#).

### WARNING

As the operations baseline is developed, refactoring may be required. Specifically, resources may later need to be [moved to a new subscription or resource group](#).

## Business continuity and disaster recovery (BCDR)

This implementation option does not implement any BCDR solution. It is assumed that the solution for protection and recover will be addressed by the development of the operations baseline.

## Assumptions

This initial blueprint assumes that the team is committed to maturing governance capabilities in parallel to the initial cloud migration efforts. If these assumptions align with your constraints, you can use the blueprint to begin the process of developing governance maturity.

- **Compliance:** No third-party compliance requirements are needed in this landing zone.
- **Limited production scope:** This landing zone could potentially host production workloads. It is not a suitable environment for sensitive data or mission-critical workloads.

If these assumptions align with your current adoption needs, then this blueprint might be a starting point for building your landing zone.

## Customize or deploy this blueprint

Learn more and download a reference sample of the CAF Foundation blueprint for deployment or customization from the Azure blueprint samples.

[Deploy the blueprint sample](#)

## Next steps

After deploying your first landing zone, you're ready to expand your landing zone.

[Expand your landing zone](#)

# Use Terraform to build your landing zones

11/9/2020 • 6 minutes to read • [Edit Online](#)

Azure provides native services for deploying your landing zones. Other third-party tools can also help with this effort. One such tool that customers and partners often use to deploy landing zones is Terraform by HashiCorp. This section shows how to use a sample landing zone to deploy foundational governance, accounting, and security capabilities for an Azure subscription.

## Purpose of the landing zone

The Cloud Adoption Framework foundations landing zone for Terraform provides features to enforce logging, accounting, and security. This landing zone uses standard components known as Terraform modules to enforce consistency across resources deployed in the environment.

## Use standard modules

Reuse of components is a fundamental principle of infrastructure as code. Modules are instrumental in defining standards and consistency across resource deployment within and across environments. The modules used to deploy this first landing zone are available in the official [Terraform registry](#).

## Architecture diagram

The first landing zone deploys the following components in your subscription:

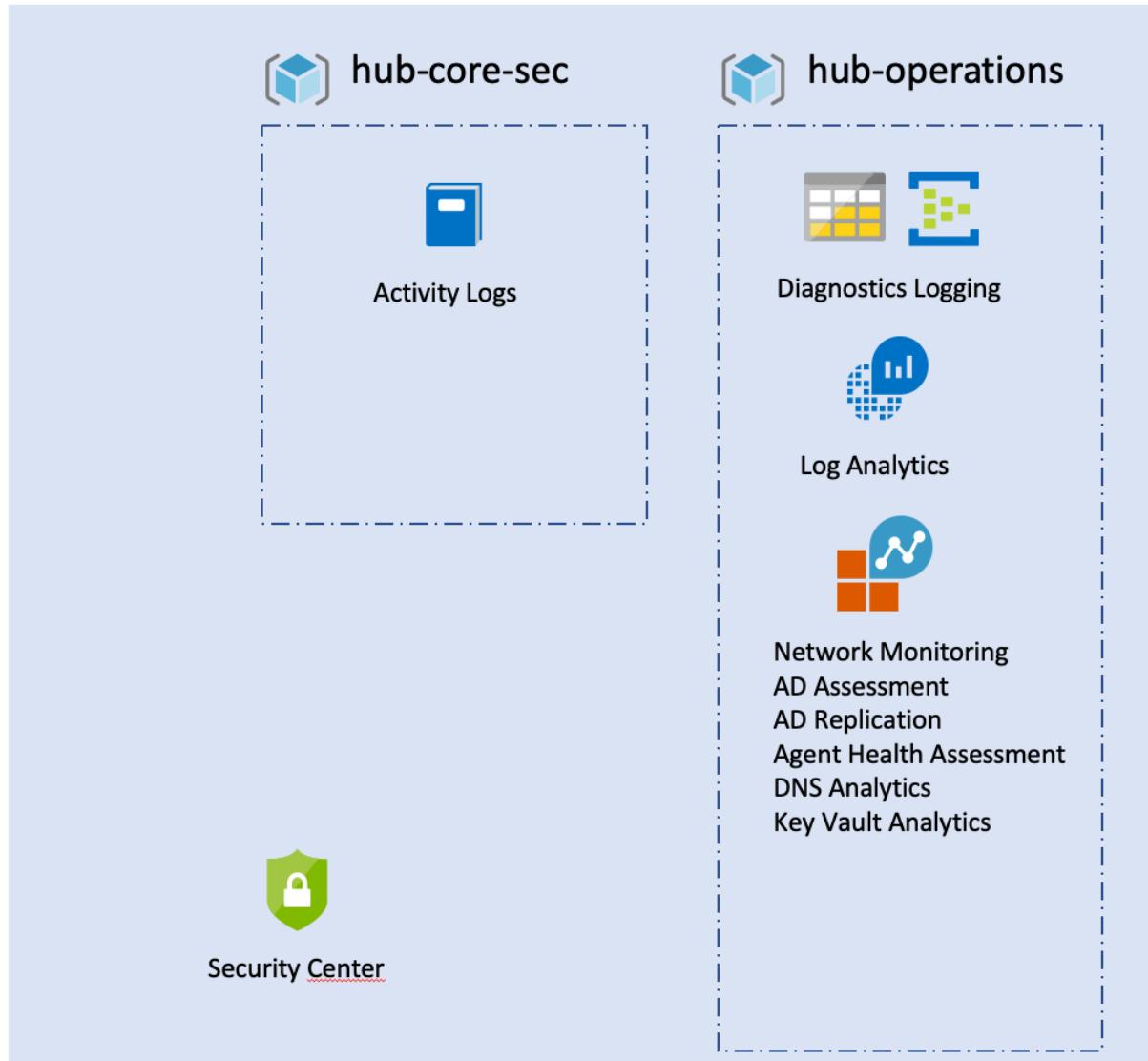


Figure 1: A foundation landing zone using Terraform.

## Capabilities

The components deployed and their purpose include the following:

COMPONENT	RESPONSIBILITY
Resource groups	Core resource groups needed for the foundation
Activity logging	Auditing all subscription activities and archiving: <ul style="list-style-type: none"> <li>Storage account</li> <li>Azure Event Hubs</li> </ul>
Diagnostics logging	All operation logs kept for a specific number of days: <ul style="list-style-type: none"> <li>Storage account</li> <li>Event Hubs</li> </ul>

COMPONENT	RESPONSIBILITY
Log Analytics	<p>Stores the operation logs. Deploy common solutions for deep application best practices review:</p> <ul style="list-style-type: none"> <li>• NetworkMonitoring</li> <li>• AdAssessment</li> <li>• AdReplication</li> <li>• AgentHealthAssessment</li> <li>• DnsAnalytics</li> <li>• KeyVaultAnalytics</li> </ul>
Azure Security Center	Security hygiene metrics and alerts sent to email and phone number

## Use this blueprint

Before you use the Cloud Adoption Framework foundation landing zone, review the following assumptions, decisions, and implementation guidance.

## Assumptions

The following assumptions or constraints were considered when this initial landing zone was defined. If these assumptions align with your constraints, you can use the blueprint to create your first landing zone. The blueprint also can be extended to create a landing zone blueprint that meets your unique constraints.

- **Subscription limits:** This adoption effort is unlikely to exceed [subscription limits](#). Two common indicators are an excess of 25,000 VMs or 10,000 vCPUs.
- **Compliance:** No third-party compliance requirements are needed for this landing zone.
- **Architectural complexity:** Architectural complexity doesn't require additional production subscriptions.
- **Shared services:** No existing shared services in Azure require this subscription to be treated like a spoke in a hub and spoke architecture.

If these assumptions match your current environment, this blueprint might be a good way to start building your landing zone.

## Design decisions

The following decisions are represented in the CAF Terraform modules:

COMPONENT	DECISIONS	ALTERNATIVE APPROACHES
Logging and monitoring	Azure Monitor Log Analytics workspace is used. A diagnostics storage account as well as event hub is provisioned.	
Network	N/A - network is implemented in another landing zone.	<a href="#">Networking decisions</a>
Identity	It's assumed that the subscription is already associated with an Azure Active Directory instance.	<a href="#">Identity management best practices</a>
Policy	This landing zone currently assumes that no Azure policies are to be applied.	

COMPONENT	DECISIONS	ALTERNATIVE APPROACHES
Subscription design	N/A - designed for a single production subscription.	<a href="#">Create initial subscriptions</a>
Resource groups	N/A - designed for a single production subscription.	<a href="#">Scale subscriptions</a>
Management groups	N/A - designed for a single production subscription.	<a href="#">Organize subscriptions</a>
Data	N/A	<a href="#">Choose the correct SQL Server option in Azure</a> and <a href="#">Azure data store guidance</a>
Storage	N/A	<a href="#">Azure Storage guidance</a>
Naming standards	When the environment is created, a unique prefix is also created. Resources that require a globally unique name (such as storage accounts) use this prefix. The custom name is appended with a random suffix. Tag usage is mandated as described in the following table.	<a href="#">Naming and tagging best practices</a>
Cost management	N/A	<a href="#">Tracking costs</a>
Compute	N/A	<a href="#">Compute options</a>

## Tagging standards

The minimum set of tags shown below must be present on all resources and resource groups:

TAG NAME	DESCRIPTION	KEY	EXAMPLE VALUES
Business unit	Top-level division of your company that owns the subscription or workload the resource belongs to.	BusinessUnit	finance, marketing, <product-name>, corp, shared
Cost center	Accounting cost center associated with this resource.	CostCenter	<cost-center-number>
Disaster recovery	Business criticality of the application, workload, or service.	DR	dr-enabled, non-dr-enabled
Environment	Deployment environment of the application, workload, or service.	Env	prod, dev, qa, staging, test, training
Owner name	Owner of the application, workload, or service.	Owner	email
Deployment type	Defines how the resources are being maintained.	DeploymentType	manual, terraform

TAG NAME	DESCRIPTION	KEY	EXAMPLE VALUES
Version	Version of the blueprint deployed.	Version	v0.1
Application name	Name of the associated application, service, or workload associated with the resource.	ApplicationName	<app-name>

## Customize and deploy your first landing zone

You can [clone your Terraform foundation landing zone](#). Get started easily with the landing zone by modifying the Terraform variables. In our example, we use `blueprint_foundations.sandbox.auto.tfvars`, so Terraform automatically sets the values in this file for you.

Let's look at the different variable sections.

In this first object, we create two resource groups in the `southeastasia` region named `-hub-core-sec` and `-hub-operations` along with a prefix added at runtime.

```
resource_groups_hub = {
    HUB-CORE-SEC      = {
        name = "-hub-core-sec"
        location = "southeastasia"
    }
    HUB-OPERATIONS   = {
        name = "-hub-operations"
        location = "southeastasia"
    }
}
```

Next, we specify the regions where we can set the foundations. Here, `southeastasia` is used to deploy all the resources.

```
location_map = {
    region1  = "southeastasia"
    region2  = "eastasia"
}
```

Then, we specify the retention period for the operations logs and the Azure subscription logs. This data is stored in separate storage accounts and an event hub, whose names are randomly generated because they must be unique.

```
azure_activity_logs_retention = 365
azure_diagnostics_logs_retention = 60
```

Into the `tags_hub`, we specify the minimum set of tags that are applied to all resources created.

```
tags_hub = {
    environment      = "DEV"
    owner            = "Arnaud"
    deploymentType   = "Terraform"
    costCenter       = "65182"
    BusinessUnit     = "SHARED"
    DR               = "NON-DR-ENABLED"
}
```

Then, we specify the Log Analytics name and a set of solutions that analyze the deployment. Here, we retained network monitoring, Active Directory assessment and replication, DNS analytics, and Key Vault analytics.

```
analytics_workspace_name = "lalogs"

solution_plan_map = {
    NetworkMonitoring = {
        "publisher" = "Microsoft"
        "product"   = "OMSGallery/NetworkMonitoring"
    },
    ADAssessment = {
        "publisher" = "Microsoft"
        "product"   = "OMSGallery/ADAssessment"
    },
    ADReplication = {
        "publisher" = "Microsoft"
        "product"   = "OMSGallery/ADReplication"
    },
    AgentHealthAssessment = {
        "publisher" = "Microsoft"
        "product"   = "OMSGallery/AgentHealthAssessment"
    },
    DnsAnalytics = {
        "publisher" = "Microsoft"
        "product"   = "OMSGallery/DnsAnalytics"
    },
    KeyVaultAnalytics = {
        "publisher" = "Microsoft"
        "product"   = "OMSGallery/KeyVaultAnalytics"
    }
}
```

Next, we configured the alert parameters for Azure Security Center.

```
# Azure Security Center Configuration
security_center = {
    contact_email   = "joe@contoso.com"
    contact_phone   = "+6500000000"
}
```

## Take action

After you've reviewed the configuration, you can deploy the configuration as you would deploy a Terraform environment. We recommend that you use the rover, which is a Docker container that allows deployment from Windows, Linux, or macOS. You can get started with the [landing zones](#).

## Next steps

The foundation landing zone lays the groundwork for a complex environment in a decomposed manner. This edition provides a set of simple capabilities that can be extended by adding other modules to the blueprint or layering additional landing zones on top of it.

Layering your landing zones is a good practice for decoupling systems, versioning each component that you're using, and allowing fast innovation and stability for your infrastructure as code deployment.

Future reference architectures will demonstrate this concept for a hub and spoke topology.

[Review the sample foundation Terraform landing zone](#)

# Expand your landing zone

11/9/2020 • 2 minutes to read • [Edit Online](#)

This section of the Ready methodology builds on the principles of [landing zone refactoring](#). As outlined in that article, a refactoring approach to infrastructure as code removes blockers to business success while minimizing risk. This series of articles assumes that you've deployed your first landing zone and would now like to expand that landing zone to meet enterprise requirements.

## Shared architecture principles

Expanding your landing zone provides a code-first approach to embedding the following principles into the landing zone and more broadly into your overall cloud environment.



Figure 1: shared architecture principles.

These same architecture principles are shared by [Azure Advisor](#), the [Microsoft Azure Well-Architected Framework](#), and the solutions in the [Azure Architecture Center](#).

## Applying these principles to your landing zone improvements

To better align with the methodologies of the Cloud Adoption Framework, the principles above are grouped into actionable landing zone improvements:

- Basic considerations: refactor a landing zone to refine hosting, fundamentals, and other foundational

elements.

- Operations expansions: add operations management configurations to improve **performance, reliability, and operational excellence**.
- Governance expansions: add governance configurations to improve **cost, reliability, security, and consistency**.
- Security expansions: add **security** configurations to improve protection of sensitive data and critical systems.

#### **WARNING**

Adoption teams who have a midterm objective (within 24 months) to host **more than 1,000 assets (apps, infrastructure, or data assets) in the cloud** should consider each of these expansions early in their cloud adoption journey. For all other adoption patterns, landing zone expansions could be a parallel iteration, allowing for early business success.

## Next steps

Before refactoring your first landing zone, it is important to understand [test-driven development of landing zones](#).

[Test-driven development of landing zones](#)

# Landing zone considerations

11/9/2020 • 2 minutes to read • [Edit Online](#)

A landing zone is the basic building block of any cloud adoption environment. The term *landing zone* refers to an environment that's been provisioned and prepared to host workloads in a cloud environment like Azure. A fully functioning landing zone is the final deliverable of any iteration of the Cloud Adoption Framework's Ready methodology.

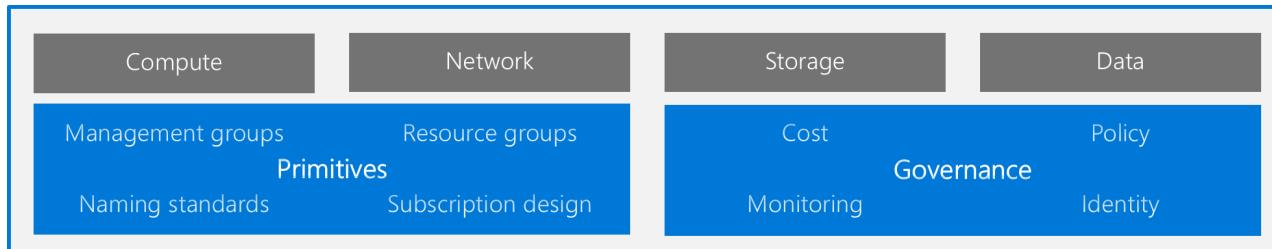


Figure 1: Landing zone considerations.

This image shows the major considerations for implementing any landing zone deployment. The considerations can be broken into three categories or types of considerations: hosting, Azure fundamentals, and governance.

## Hosting considerations

All landing zones provide structure for hosting options. The structure is created explicitly through governance controls or organically through the adoption of services within the landing zone. The following articles can help you make decisions that will be reflected in the blueprint or other automation scripts that create your landing zone:

- **Compute decisions:** To minimize operational complexity, align compute options with the purpose of the landing zone. This decision can be enforced by using automation toolchains like Azure Policy initiatives and landing zones.
- **Storage decisions:** Choose the right Azure Storage solution to support your workload requirements.
- **Networking decisions:** Choose networking services, tools, and architectures to support your organization's workload, governance, and connectivity requirements.
- **Database decisions:** Determine which database technology is best suited for your workload requirements.

## Azure fundamentals

Each landing zone is part of a broader solution for organizing resources across a cloud environment. Azure fundamentals are the foundational building blocks for an organization.

- **Azure fundamental concepts:** Learn fundamental concepts and terms that are used to organize resources in Azure and how the concepts relate to one another.
- **Resource consistency decision guide:** When you understand each of the fundamentals, the resource organization decision guide can help you make decisions that shape the landing zone.

## Governance considerations

The Cloud Adoption Framework's Govern methodologies establish a process for governing the environment as a whole. Many use cases might require you to make governance decisions on a per-landing-zone basis. In many scenarios, governance baselines are enforced on a per-landing-zone basis even though the baselines are established holistically. It's true for the first few landing zones that an organization deploys.

The following articles can help you make governance-related decisions about your landing zone. You can factor each decision into your governance baselines.

- **Cost requirements.** Based on an organization's motivation for cloud adoption and operational commitments made about its environment, various cost management configurations might need to be changed for the landing zone.
- **Monitoring decisions.** Depending on the operational requirements for a landing zone, various monitoring tools can be deployed. The monitoring decisions article can help you determine the most appropriate tools to deploy.
- **Role-based access control.** Azure [role-based access control \(RBAC\)](#) offers fine-grained, group-based access management for resources that are organized around user roles.
- **Policy decisions.** [Azure Blueprints samples](#) provide premade compliance blueprints, each with predefined policy initiatives. Policy decisions help inform a selection of the best blueprint or policy initiative based on your requirements and constraints.
- **Create hybrid cloud consistency.** Create hybrid cloud solutions that give your organization the benefits of cloud innovation while maintaining many of the conveniences of on-premises management.

# Review your compute options

11/9/2020 • 6 minutes to read • [Edit Online](#)

Determining the compute requirements for hosting your workloads is a key consideration as you prepare for your cloud adoption. Azure compute products and services support a wide variety of workload computing scenarios and capabilities. How you configure your landing zone environment to support your compute requirements depends on your workload's governance, technical, and business requirements.

## Identify compute services requirements

As part of your landing zone evaluation and preparation, you need to identify all compute resources that your landing zone will need to support. This process involves assessing each of the applications and services that make up your workloads to determine your compute and hosting requirements. After you identify and document your requirements, you can create policies for your landing zone to control what resource types are allowed based on your workload needs.

For each application or service you'll deploy to your landing zone environment, use the following decision tree as a starting point to help you determine your compute services requirements:

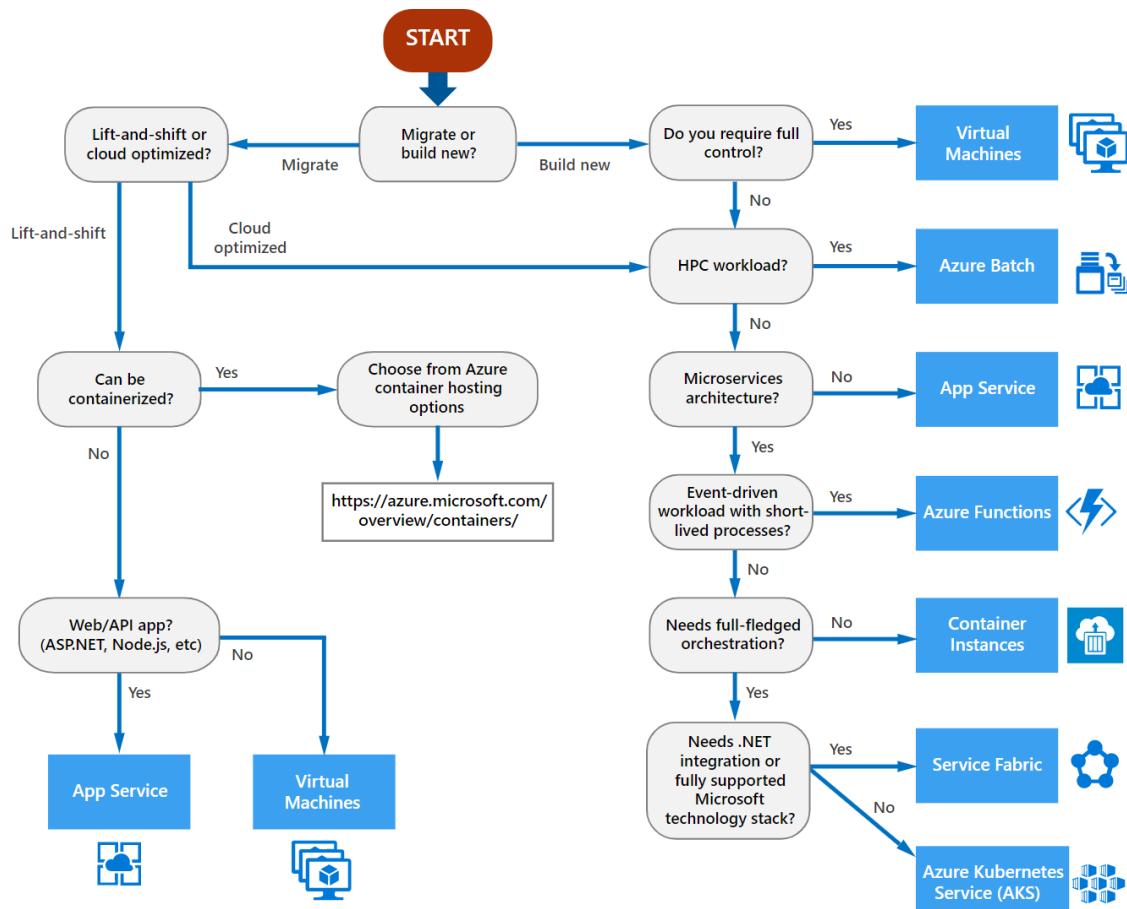


Figure 1: An Azure compute services decision tree.

### NOTE

Learn more about how to assess compute options for each of your applications or services in the [Azure application architecture guide](#).

## Key questions

Answer the following questions about your workloads to help you make decisions based on the Azure compute services decision tree:

- **Are you building net-new applications and services or migrating from existing on-premises workloads?** Developing new applications as part of your cloud adoption efforts allows you to take full advantage of modern cloud-based hosting technologies from the design phase moving forward.
- **If you're migrating existing workloads, can they take advantage of modern cloud technologies?** Migrating on-premises workloads requires analysis. Can you easily optimize existing applications and services to take advantage of modern cloud technologies, or will a lift-and-shift approach work better for your workloads?
- **Can your applications or services take advantage of containers?** If your applications are good candidates for containerized hosting, you can take advantage of the resource efficiency, scalability, and orchestration capabilities provided by [container services in Azure](#). Both [Azure managed disks](#) and [Azure Files](#) can be used for persistent storage in containerized applications.
- **Are your applications web- or API-based, and do they use PHP, ASP.NET, Node.js, or similar technologies?** Web apps can be deployed to managed [Azure App Service](#) instances, so you don't have to maintain virtual machines for hosting purposes.
- **Will you require full control over the OS and hosting environment of your workload?** If you need to control the hosting environment, including OS, disks, locally running software, and other configurations, you can use [Azure Virtual Machines](#) to host your applications and services. In addition to choosing your virtual machine sizes and performance tiers, your decisions regarding virtual disk storage will affect performance and SLAs related to your infrastructure-as-a-service workloads. For more information, see the [Azure disk storage](#) documentation.
- **Will your workload involve high-performance computing (HPC) capabilities?** [Azure Batch](#) provides job scheduling and autoscaling of compute resources as a platform service, so it's easy to run large-scale parallel and HPC applications in the cloud.
- **Will your applications use a microservices architecture?** Applications that use a microservices-based architecture can take advantage of several optimized compute technologies. Self-contained, event-driven workloads can use [Azure Functions](#) to build scalable, serverless applications that don't need an infrastructure. For applications that require more control over the environment where microservices run, you can use container services like [Azure container instances](#), [Azure Kubernetes Service](#), and [Azure Service Fabric](#).

### NOTE

Most Azure compute services are used in combination with Azure Storage. Consult the [storage decisions guidance](#) for related storage decisions.

## Common compute scenarios

The following table illustrates a few common use scenarios and the recommended compute services for handling them:

SCENARIO	COMPUTE SERVICE
I need to provision Linux and Windows virtual machines in seconds with the configurations of my choice.	<a href="#">Azure Virtual Machines</a>
I need to achieve high availability by autoscaling to create thousands of VMs in minutes.	<a href="#">Virtual machine scale sets</a>

SCENARIO	COMPUTE SERVICE
I want to simplify the deployment, management, and operations of Kubernetes.	<a href="#">Azure Kubernetes Service (AKS)</a>
I need to accelerate app development by using an event-driven serverless architecture.	<a href="#">Azure Functions</a>
I need to develop microservices and orchestrate containers on Windows and Linux.	<a href="#">Azure Service Fabric</a>
I want to quickly create cloud apps for web and mobile by using a fully managed platform.	<a href="#">Azure App Service</a>
I want to containerize apps and easily run containers by using a single command.	<a href="#">Azure container instances</a>
I need cloud-scale job scheduling and compute management with the ability to scale to tens, hundreds, or thousands of virtual machines.	<a href="#">Azure Batch</a>
I need to create highly available, scalable cloud applications and APIs that can help me focus on apps instead of hardware.	<a href="#">Azure cloud services</a>

## Regional availability

Azure lets you deliver services at the scale you need to reach your customers and partners **wherever they are**. A key factor in planning your cloud deployment is to determine which Azure region will host your workload resources.

Some compute options such as Azure App Service are generally available in most Azure regions while other compute services are supported only in certain regions. Some virtual machine types and their associated storage types have limited regional availability. Before you decide the regions to which you will deploy your compute resources, we recommend that you refer to the [regions page](#) to check the latest status of regional availability.

To learn more about the Azure global infrastructure, see the [Azure regions page](#). You can also view [products available by region](#) for specific details about the overall services that are available in each Azure region.

## Data residency and compliance requirements

Legal and contractual requirements related to data storage often will apply to your workloads. These requirements might vary based on the location of your organization, the jurisdiction where files and data are stored and processed, and your applicable business sector. Components of data obligations to consider include data classification, data location, and the respective responsibilities for data protection under the shared responsibility model. Many compute solutions depend on linked storage resources. This requirement also might influence your compute decisions. For help with understanding these requirements, see the white paper [achieving compliant data residency and security with Azure](#).

Part of your compliance efforts might include controlling where your compute resources are physically located. Azure regions are organized into groups called geographies. An [Azure geography](#) ensures that data residency, sovereignty, compliance, and resiliency requirements are honored within geographical and political boundaries. If your workloads are subject to data sovereignty or other compliance requirements, you must deploy your storage resources to regions in a compliant Azure geography.

## Establish controls for compute services

When you prepare your landing zone environment, you can establish controls that limit what resources each user can deploy. The controls can help you manage costs and limit security risks while still allowing developers and IT teams to deploy and configure resources that are needed to support your workloads.

After you identify and document your landing zone's requirements, you can use [Azure Policy](#) to control the compute resources that you allow users to create. Controls can take the form of [allowing or denying the creation of compute resource types](#). For example, you might restrict users to creating only Azure App Service or Azure Functions resources. You also can use policy to control the allowable options when a resource is created, like [restricting what virtual machine SKUs can be provisioned](#) or [allowing only specific VM images](#).

Policies can be scoped to resources, resource groups, subscriptions, and management groups. You can include your policies in [Azure blueprint](#) definitions and apply them repeatedly throughout your cloud estate.

# Review your network options

11/9/2020 • 7 minutes to read • [Edit Online](#)

Designing and implementing Azure networking capabilities is a critical part of your cloud adoption efforts. You'll need to make networking design decisions to properly support the workloads and services that will be hosted in the cloud. Azure networking products and services support a wide variety of networking capabilities. How you structure these services and the networking architectures you choose depends on your organization's workload, governance, and connectivity requirements.

## Identify workload networking requirements

As part of your landing zone evaluation and preparation, you need to identify the networking capabilities that your landing zone needs to support. This process involves assessing each of the applications and services that make up your workloads to determine their connectivity network control requirements. After you identify and document the requirements, you can create policies for your landing zone to control the allowed networking resources and configuration based on your workload needs.

For each application or service you'll deploy to your landing zone environment, use the following decision tree as a starting point to help you determine the networking tools or services to use:

# CAF Ready

## Networking decision tree

This decision tree serves to guide high-level initial decisions. A deep understanding of business motivations, technology strategy, timeline, and landing zone design is required to validate these decisions.

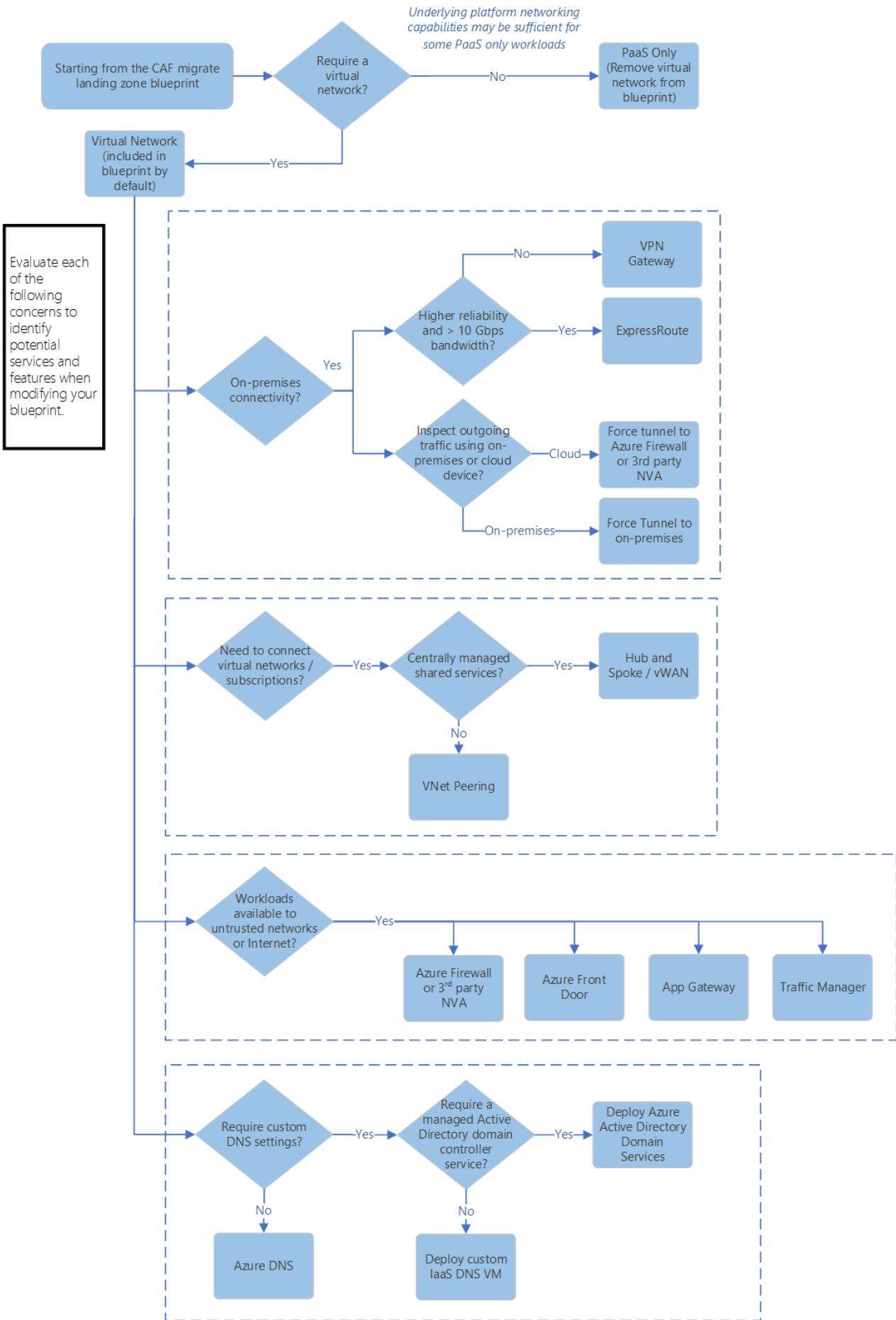


Figure 1: The Azure networking service decision tree.

## Key questions

Answer the following questions about your workloads to help you make decisions based on the Azure networking services decision tree:

- **Will your workloads require a virtual network?** Managed platform as a service (PaaS) resource types use underlying platform network capabilities that don't always require a virtual network. If your workloads don't require advanced networking features and you don't need to deploy infrastructure as a service (IaaS) resources, the default [native networking capabilities provided by PaaS resources](#) might meet your workload connectivity and traffic management requirements.
- **Will your workloads require connectivity between virtual networks and your on-premises datacenter?** Azure provides two solutions for establishing hybrid networking capabilities: Azure VPN gateway and Azure ExpressRoute. [Azure VPN gateway](#) connects your on-premises networks to Azure through site-to-site VPNs similar to how you might set up and connect to a remote branch office. VPN gateway has a maximum bandwidth of 10 Gbps. [Azure ExpressRoute](#) offers higher reliability and lower latency by using a private connection between Azure and your on-premises infrastructure. Bandwidth options for ExpressRoute range from 50 Mbps to 100 Gbps.
- **Will you need to inspect and audit outgoing traffic by using on-premises network devices?** For cloud-native workloads, you can use [Azure Firewall](#) or cloud-hosted, third-party [network virtual appliances \(NVAs\)](#) to inspect and audit traffic moving to or from the public internet. But many enterprise IT security policies require internet-bound outgoing traffic to pass through centrally managed devices in the organization's on-premises environment. [Forced tunneling](#) supports these scenarios. Not all managed services support forced tunneling. Services and features like [App Service Environment in Azure App Service](#), [Azure API management](#), [Azure Kubernetes Service \(AKS\)](#), [Azure SQL Managed Instance](#), [Azure Databricks](#), and [Azure HDInsight](#) support this configuration when the service or feature is deployed inside a virtual network.
- **Do you need to connect multiple virtual networks?** You can use [virtual network peering](#) to connect multiple instances of [Azure Virtual Network](#). Peering can support connections across subscriptions and regions. For scenarios where you provide services that are shared across multiple subscriptions or need to manage a large number of network peerings, consider adopting a [hub and spoke networking architecture](#) or using [Azure Virtual WAN](#). Virtual network peering provides connectivity only between two peered networks. By default, it doesn't provide transitive connectivity across multiple peerings.
- **Will your workloads be accessible over the internet?** Azure provides services that are designed to help you manage and secure external access to your applications and services:
  - [Azure Firewall](#)
  - [Network appliances](#)
  - [Azure Front Door](#)
  - [Azure Application Gateway](#)
  - [Azure Traffic Manager](#)
- **Will you need to support custom DNS management?** [Azure DNS](#) is a hosting service for DNS domains. Azure DNS provides name resolution by using the Azure infrastructure. If your workloads require name resolution that goes beyond the features that are provided by Azure DNS, you might need to deploy additional solutions. If your workloads also require Active Directory services, consider using [Azure Active Directory Domain Services](#) to augment Azure DNS capabilities. For more capabilities, you can also [deploy custom IaaS virtual machines](#) to support your requirements.

## Common networking scenarios

Azure networking is composed of multiple products and services that provide different networking capabilities. As part of your networking design process, you can compare your workload requirements to the networking scenarios in the following table to identify the Azure tools or services you can use to provide these networking capabilities:

SCENARIO	NETWORKING PRODUCT OR SERVICE
I need the networking infrastructure to connect everything, from virtual machines to incoming VPN connections.	<a href="#">Azure Virtual Network</a>
I need to balance inbound and outbound connections and requests to my applications or services.	<a href="#">Azure Load Balancer</a>
I want to optimize delivery from application server farms while increasing application security with a Web Application Firewall.	<a href="#">Azure Application Gateway</a> <a href="#">Azure Front Door</a>
I need to securely use the internet to access Azure Virtual Network through high-performance VPN gateways.	<a href="#">Azure VPN gateway</a>
I want to ensure ultra-fast DNS responses and ultra-high availability for all my domain needs.	<a href="#">Azure DNS</a>
I need to accelerate the delivery of high-bandwidth content to customers worldwide, from applications and stored content to streaming video.	<a href="#">Azure Content Delivery Network (CDN)</a>
I need to protect my Azure applications from DDoS attacks.	<a href="#">Azure DDoS protection</a>
I need to distribute traffic optimally to services across global Azure regions, while providing high availability and responsiveness.	<a href="#">Azure Traffic Manager</a> <a href="#">Azure Front Door</a>
I need to add private network connectivity to access Microsoft cloud services from my corporate networks, as if they were on-premises and residing in my own datacenter.	<a href="#">Azure ExpressRoute</a>
I want to monitor and diagnose conditions at a network-scenario level.	<a href="#">Azure Network Watcher</a>
I need native firewall capabilities, with built-in high availability, unrestricted cloud scalability, and zero maintenance.	<a href="#">Azure Firewall</a>
I need to connect business offices, retail locations, and sites securely.	<a href="#">Azure Virtual WAN</a>
I need a scalable, security-enhanced delivery point for global microservices-based web applications.	<a href="#">Azure Front Door</a>

## Choose a networking architecture

After you identify the Azure networking services that you need to support your workloads, you also need to design the architecture that will combine these services to provide your landing zone's cloud networking infrastructure. The Cloud Adoption Framework [Software Defined Networking decision guide](#) provides details about some of the most common networking architecture patterns used on Azure.

The following table summarizes the primary scenarios that these patterns support:

SCENARIO	SUGGESTED NETWORK ARCHITECTURE
All of the Azure-hosted workloads deployed to your landing zone will be entirely PaaS-based, won't require a virtual network, and aren't part of a wider cloud adoption effort that includes IaaS resources.	PaaS-only
Your Azure-hosted workloads will deploy IaaS-based resources like virtual machines or otherwise require a virtual network, but don't require connectivity to your on-premises environment.	Cloud-native
Your Azure-hosted workloads require limited access to on-premises resources, but you're required to treat cloud connections as untrusted.	Cloud DMZ
Your Azure-hosted workloads require limited access to on-premises resources, and you plan to implement mature security policies and secure connectivity between the cloud and your on-premises environment.	Hybrid
You need to deploy and manage a large number of VMs and workloads, potentially exceeding <a href="#">Azure subscription limits</a> , you need to share services across subscriptions, or you need a more segmented structure for role, application, or permission segregation.	Hub and spoke
You have many branch offices that need to connect to each other and to Azure.	Azure Virtual WAN

## Azure Virtual Datacenter

In addition using one of these architecture patterns, if your enterprise IT group manages large cloud environments, consider consulting the [CAF enterprise-scale landing zone](#). When you design your Azure-based cloud infrastructure, the CAF enterprise-scale landing zone provides a combined approach to networking, security, management, and infrastructure if you have a mid-term objective (within 24 months) to **host more than 1,000 assets (apps, infrastructure, or data assets) in the cloud**.

For organizations that meet the following criteria, you may also want to start with the [CAF enterprise-scale landing zone](#):

- Your enterprise is subject to regulatory compliance requirements that require centralized monitoring and audit capabilities.
- You need to maintain common policy and governance compliance and centralized IT control over core services.
- Your industry depends on a complex platform which requires complex controls and deep domain expertise to govern the platform. This is most common in large enterprises within finance, oil and gas, or manufacturing.
- Your existing IT governance policies require tighter parity with existing features, even during early stage adoption.

## Follow Azure networking best practices

As part of your networking design process, see these articles:

- [Virtual network planning](#). Learn how to plan for virtual networks based on your isolation, connectivity, and location requirements.
- [Azure best practices for network security](#). Learn about Azure best practices that can help you enhance your network security.

- [Best practices for networking when you migrate workloads to Azure](#). Get additional guidance about how to implement Azure networking to support IaaS-based and PaaS-based workloads.

# Review your storage options

11/9/2020 • 17 minutes to read • [Edit Online](#)

Storage capabilities are critical for supporting workloads and services that are hosted in the cloud. As part of your cloud adoption readiness preparations, review this article to help you plan for and address your storage needs.

## Select storage tools and services to support your workloads

[Azure Storage](#) is the Azure platform's managed service for providing cloud storage. Azure Storage is composed of several core services and supporting features. Storage in Azure is highly available, secure, durable, scalable, and redundant. Review the scenarios and considerations described here to choose the relevant Azure services and the correct architectures to fit your organization's workload, governance, and data storage requirements.

### Key questions

Answer the following questions about your workloads to help you make decisions based on the Azure Storage decision tree:

- **Do your workloads require disk storage to support the deployment of infrastructure as a service (IaaS) virtual machines?** [Azure disk storage](#) provides virtual disk capabilities for IaaS virtual machines.
- **Will you need to provide downloadable images, documents, or other media as part of your workloads?** [Azure Blob storage](#) provides the ability to [host static files](#), which are then accessible for download over the internet. You can make assets that are hosted in Blob storage public, or you can [limit assets to authorized users](#) via Azure Active Directory (Azure AD), shared keys, or shared access signatures.
- **Will you need a location to store virtual machine logs, application logs, and analytics data?** You can use Azure Blob storage to [store Azure Monitor log data](#).
- **Will you need to provide a location for backup, disaster recovery, or archiving workload-related data?** Azure disk storage uses Azure Blob storage to provide [backup and disaster recovery capabilities](#). You can also use Blob storage as a location to back up other resources, like on-premises or IaaS VM-hosted [SQL Server data](#).
- **Will you need to support big data analytics workloads?** [Azure Data Lake Storage gen 2](#) is built on top of Azure Blob storage. Data Lake Storage gen 2 can support large-enterprise data lake functionality. It also can handle storing petabytes of information while sustaining hundreds of gigabits of throughput.
- **Will you need to provide cloud-native file shares?** Azure has two primary services that provide cloud-hosted file shares: Azure NetApp Files and Azure Files. [Azure NetApp Files](#) provides high-performance NFS shares that are well suited to common enterprise workloads like SAP. [Azure Files](#) provides file shares accessible over SMB 3.0 and HTTPS.
- **Will you need to support hybrid cloud storage for on-premises high-performance computing (HPC) workloads?** [Avere vFXT for Azure](#) is a hybrid caching solution that you can use to expand your on-premises storage capabilities by using cloud-based storage. Avere vFXT for Azure is optimized for read-heavy HPC workloads that involve compute farms of 1,000 to 40,000 CPU cores. Avere vFXT for Azure can integrate with on-premises hardware network attached storage (NAS), Azure Blob storage, or both.
- **Will you need to perform large-scale archiving and syncing of your on-premises data to the cloud?** [Azure Data Box](#) products are designed to help you move large amounts of data from your on-premises environment to the cloud. [Azure Data Box Gateway](#) is a virtual device that resides on-premises. Data Box Gateway helps you manage large-scale data migration to the cloud. If you need to analyze, transform, or filter data before you move it to the cloud, you can use [Azure Data Box Edge](#), an AI-enabled physical edge computing device that's deployed to your on-premises environment. Data Box Edge accelerates processing and the secure transfer of data to Azure.

- Do you want to expand an existing on-premises file share to use cloud storage? [Azure file sync](#) lets you use the Azure Files service as an extension of file shares that are hosted on your on-premises Windows server machines. The syncing service transforms Windows server into a quick cache of your Azure file share. It allows your on-premises machines that access the share to use any protocol that's available on Windows server.

## Common storage scenarios

Azure offers multiple products and services for different storage capabilities. In addition to the storage requirements decision tree shown earlier, the following table describes a-series of potential storage scenarios and the recommended Azure services to address the scenario's requirements.

### Block storage scenarios

SCENARIO	SUGGESTED AZURE SERVICES	CONSIDERATIONS FOR SUGGESTED SERVICES
I have bare-metal servers or VMs (Hyper-V or VMware) with direct attached storage running LOB applications.	<a href="#">Azure disk storage (premium SSD)</a>	For production services, the premium SSD option provides consistent low-latency coupled with high IOPS and throughput.
I have servers that will host web and mobile apps.	<a href="#">Azure disk storage (standard SSD)</a>	standard SSD IOPS and throughput might be sufficient (at a lower cost than premium SSD) for CPU-bound web and app servers in production.
I have an enterprise SAN or all-flash array.	<a href="#">Azure disk storage (premium or ultra SSD)</a>  <a href="#">Azure NetApp Files</a>	ultra SSD is NVMe-based and offers submillisecond latency with high IOPS and bandwidth. ultra SSD is scalable up to 64 TB. The choice of premium SSD and ultra SSD depends on peak latency, IOPS, and scalability requirements.
I have high-availability (HA) clustered servers (such as SQL Server FCI or Windows server failover clustering).	<a href="#">Azure Files (premium)</a>  <a href="#">Azure disk storage (premium or ultra SSD)</a>	Clustered workloads require multiple nodes to mount the same underlying shared storage for failover or HA. Premium file shares offer shared storage that's mountable via SMB. Shared block storage also can be configured on premium SSD or ultra SSD by using <a href="#">partner solutions</a> .
I have a relational database or data warehouse workload (such as SQL Server or Oracle).	<a href="#">Azure disk storage premium or ultra SSD</a>	The choice of premium SSD versus ultra SSD depends on peak latency, IOPS, and scalability requirements. ultra SSD also reduces complexity by <a href="#">removing the need for storage pool configuration for scalability</a> .
I have a NoSQL cluster (such as Cassandra or MongoDB).	<a href="#">Azure disk storage (premium SSD)</a>	Azure disk storage premium SSD offering provides consistent low-latency coupled with high IOPS and throughput.

SCENARIO	SUGGESTED AZURE SERVICES	CONSIDERATIONS FOR SUGGESTED SERVICES
I am running containers with persistent volumes.	<a href="#">Azure Files (standard or premium)</a>  <a href="#">Azure disk storage (standard, premium, or ultra SSD)</a>	File (RWX) and block (RWO) volumes driver options are available for both Azure Kubernetes Service (AKS) and custom Kubernetes deployments. Persistent volumes can map to either an Azure disk storage disk or a managed Azure Files share. Choose premium versus standard options bases on workload requirements for persistent volumes.
I have a data lake (such as a Hadoop cluster for HDFS data).	<a href="#">Azure Data Lake Storage gen 2</a>  <a href="#">Azure disk storage (standard or premium SSD)</a>	The Data Lake Storage gen 2 feature of Azure Blob storage provides server-side HDFS compatibility and petabyte scale for parallel analytics. It also offers HA and reliability. Software like Cloudera can use premium or standard SSD on master/worker nodes, if needed.
I have an SAP or SAP HANA deployment.	<a href="#">Azure disk storage (premium or ultra SSD)</a>	ultra SSD is optimized to offer submillisecond latency for tier-1 SAP workloads. ultra SSD is now in preview. premium SSD coupled with M-series VMs offers a general-availability option.
I have a disaster recovery site with strict RPO/RTO that syncs from my primary servers.	<a href="#">Azure page blobs</a>	Azure page blobs are used by replication software to enable low-cost replication to Azure without the need for compute VMs until failover occurs. For more information, see the <a href="#">Azure disk storage documentation</a> . Note: Page blobs support a maximum of 8 TB.

## File and object storage scenarios

SCENARIO	SUGGESTED AZURE SERVICES	CONSIDERATIONS FOR SUGGESTED SERVICES
I use Windows file server.	<a href="#">Azure Files</a>  <a href="#">Azure file sync</a>	With Azure file sync, you can store rarely used data on cloud-based Azure file shares while caching your most frequently used files on-premises for fast, local access. You can also use multisite sync to keep files in sync across multiple servers. If you plan to migrate your workloads to a cloud-only deployment, Azure Files might be sufficient.

SCENARIO	SUGGESTED AZURE SERVICES	CONSIDERATIONS FOR SUGGESTED SERVICES
I have an enterprise NAS (such as Azure NetApp Files or Dell-EMC Isilon).	<a href="#">Azure NetApp Files</a> <a href="#">Azure Files (premium)</a>	If you have an on-premises deployment of NetApp, consider using Azure NetApp Files to migrate your deployment to Azure. If you're using or migrating to a Windows or Linux server, or you have basic file-share needs, consider using Azure Files. For continued on-premises access, use Azure file sync to sync Azure file shares with on-premises file shares by using a cloud-tiering mechanism.
I have a file share (SMB or NFS).	<a href="#">Azure Files (standard or premium)</a> <a href="#">Azure NetApp Files</a>	The choice of premium versus standard Azure Files tiers depends on IOPS, throughput, and your need for latency consistency. If you have an on-premises deployment of NetApp, consider using Azure NetApp Files. If you need to migrate your access control lists (ACLs) and timestamps to the cloud, Azure file sync can bring all these settings to your Azure file shares as a convenient migration path.
I have an on-premises object storage system for petabytes of data (such as Dell-EMC ECS).	<a href="#">Azure Blob storage</a>	Azure Blob storage provides premium, hot, cool, and archive tiers to match your workload performance and cost needs.
I have a DFSR deployment or another way of handling branch offices.	<a href="#">Azure Files</a> <a href="#">Azure file sync</a>	Azure file sync offers multisite sync to keep files in sync across multiple servers and native Azure file shares in the cloud. Move to a fixed storage footprint on-premises by using cloud tiering. Cloud tiering transforms your server into a cache for the relevant files while scaling cold data in Azure file shares.
I have a tape library (either on-premises or offsite) for backup and disaster recovery or long-term data retention.	<a href="#">Azure Blob storage (cool or archive tiers)</a>	An Azure Blob storage archive tier will have the lowest possible cost, but it might require hours to copy the offline data to a cool, hot, or Premium tier of storage to allow access. Cool tiers provide instantaneous access at low cost.

SCENARIO	SUGGESTED AZURE SERVICES	CONSIDERATIONS FOR SUGGESTED SERVICES
I have file or object storage configured to receive my backups.	<a href="#">Azure Blob storage (cool or archive tiers)</a> <a href="#">Azure file sync</a>	To back up data for long-term retention with lowest-cost storage, move data to Azure Blob storage and use cool and archive tiers. To enable fast disaster recovery for file data on a server (on-premises or in an Azure VM), sync shares to individual Azure file shares by using Azure file sync. With Azure file share snapshots, you can restore earlier versions and sync them back to connected servers or access them natively in the Azure file share.
I run data replication to a disaster recovery site.	<a href="#">Azure Files</a> <a href="#">Azure file sync</a>	Azure file sync removes the need for a disaster recovery server and stores files in native Azure SMB shares. Fast disaster recovery rebuilds any data on a failed on-premises server quickly. You can even keep multiple server locations in sync or use cloud tiering to store only relevant data on-premises.
I manage data transfer in disconnected scenarios.	<a href="#">Azure Data Box Edge or Azure Data Box Gateway</a>	Using Data Box Edge or Data Box Gateway, you can copy data in disconnected scenarios. When the gateway is offline, it saves all files you copy in the cache, then uploads them when you're connected.
I manage an ongoing data pipeline to the cloud.	<a href="#">Azure Data Box Edge or Azure Data Box Gateway</a>	Move data to the cloud from systems that are constantly generating data just by having them copy that data straight to the storage gateway. If they need to access that data later, it's right there where they put it.
I have bursts of quantities of data that arrive at the same time.	<a href="#">Azure Data Box Edge or Azure Data Box Gateway</a>	Manage large quantities of data that arrive at the same time, like when an autonomous car pulls back into the garage, or a gene sequencing machine finishes its analysis. Copy all that data to Data Box Gateway at fast local speeds, and then let the gateway upload it as your network allows.

## Plan based on data workloads

SCENARIO	SUGGESTED AZURE SERVICES	CONSIDERATIONS FOR SUGGESTED SERVICES
I want to develop a new cloud-native application that needs to persist unstructured data.	<a href="#">Azure Blob storage</a>	
I need to migrate data from an on-premises NetApp instance to Azure.	<a href="#">Azure NetApp Files</a>	

SCENARIO	SUGGESTED AZURE SERVICES	CONSIDERATIONS FOR SUGGESTED SERVICES
I need to migrate data from on-premises Windows file server instances to Azure.	<a href="#">Azure Files</a>	
I need to move file data to the cloud but continue to primarily access the data from on-premises.	<a href="#">Azure Files</a> <a href="#">Azure file sync</a>	
I need to support "burst compute" - NFS/SMB read-heavy, file-based workloads with data assets that reside on-premises while computation runs in the cloud.	<a href="#">Avere vFXT for Azure</a>	IaaS scale-out NFS/SMB file caching
I need to move an on-premises application that uses a local disk or iSCSI.	<a href="#">Azure disk storage</a>	
I need to migrate a container-based application that has persistent volumes.	<a href="#">Azure disk storage</a> <a href="#">Azure Files</a>	
I need to move file shares that aren't Windows server or NetApp to the cloud.	<a href="#">Azure Files</a> <a href="#">Azure NetApp Files</a>	Protocol support regional availability performance requirements snapshot and clone capabilities price sensitivity
I need to transfer terabytes to petabytes of data from on-premises to Azure.	<a href="#">Azure Data Box Edge</a>	
I need to process data before transferring it to Azure.	<a href="#">Azure Data Box Edge</a>	
I need to support continuous data ingestion in an automated way by using local cache.	<a href="#">Azure Data Box Gateway</a>	

## Learn more about Azure Storage services

After you identify the Azure tools that best match your requirements, use the detailed documentation linked in the following table to familiarize yourself with these services:

SERVICE	DESCRIPTION

SERVICE	DESCRIPTION
Azure Blob storage	<p>Azure Blob storage is Microsoft's object storage solution for the cloud. Blob storage is optimized for storing massive amounts of unstructured data. Unstructured data is data that doesn't adhere to a specific data model or definition, such as text or binary data.</p> <p>Blob storage is designed for:</p> <ul style="list-style-type: none"> <li>• Serving images or documents directly to a browser.</li> <li>• Storing files for distributed access.</li> <li>• Streaming video and audio.</li> <li>• Writing to log files.</li> <li>• Storing data for backup and restore, disaster recovery, and archiving.</li> <li>• Storing data for analysis by an on-premises or Azure-hosted service.</li> </ul>
Azure Data Lake Storage gen 2	<p>Blob storage supports Azure Data Lake Storage Gen2, Microsoft's enterprise big data analytics solution for the cloud. Azure Data Lake Storage Gen2 offers a hierarchical file system as well as the advantages of Blob storage, including low-cost, tiered storage; high availability; strong consistency; and disaster recovery capabilities.</p>
Azure disk storage	<p>Azure disk storage offers persistent, high-performance block storage to power Azure Virtual Machines. Azure disks are highly durable, secure, and offer the industry's only single-instance SLA for VMs that use <a href="#">premium or ultra SSDs</a>. Azure disks provide high availability with availability sets and availability zones that map to your Azure Virtual Machines fault domains. In addition, Azure disks are managed as a top-level resource in Azure. Azure Resource Manager capabilities like role-based access control (RBAC), policy, and tagging by default are provided.</p>
Azure Files	<p>Azure Files provides fully managed, native SMB file shares, without the need to run a VM. You can mount an Azure Files share as a network drive to any Azure VM or on-premises machine.</p>
Azure file sync	<p>Azure file sync can be used to centralize your organization's file shares in Azure Files, while keeping the flexibility, performance, and compatibility of an on-premises file server. Azure file sync transforms Windows server into a quick cache of your Azure file share.</p>
Azure NetApp Files	<p>The Azure NetApp Files service is an enterprise-class, high-performance, metered file storage service. Azure NetApp Files supports any workload type and is highly available by default. You can select service and performance levels and set up snapshots through the service.</p>
Azure Data Box Edge	<p>Azure Data Box Edge is an on-premises network device that moves data into and out of Azure. Data Box Edge has AI-enabled edge compute to preprocess data during upload. Data Box Gateway is a virtual version of the device but with the same data transfer capabilities.</p>

SERVICE	DESCRIPTION
Azure Data Box Gateway	Azure Data Box Gateway is a storage solution that enables you to seamlessly send data to Azure. Data Box Gateway is a virtual device based on a virtual machine provisioned in your virtualized environment or hypervisor. The virtual device resides on-premises and you write data to it by using the NFS and SMB protocols. The device then transfers your data to Azure block blobs or Azure page blobs, or to Azure Files.
Avere vFXT for Azure	Avere vFXT for Azure is a filesystem caching solution for data-intensive high-performance computing (HPC) tasks. Take advantage of cloud computing's scalability to make your data accessible when and where it's needed, even for data that's stored in your own on-premises hardware.

## Data redundancy and availability

Azure Storage has various redundancy options to help ensure durability and high availability based on customer needs: locally redundant storage, zone-redundant storage, geo-redundant storage (GRS), and read-access GRS (RA-GRS).

See [Azure Storage redundancy](#) to learn more about these capabilities and how you can decide on the best redundancy option for your use cases. Also, service-level agreements (SLAs) for storage services provide guarantees that are financially backed. For more information, see [SLA for managed disks](#), [SLA for virtual machines](#), and [SLA for storage accounts](#).

For help with planning the right solution for Azure disks, see [Backup and disaster recovery for Azure disk storage](#).

## Security

To help you protect your data in the cloud, Azure Storage offers several best practices for data security and encryption for data at rest and in transit. You can:

- Secure the storage account by using RBAC and Azure AD.
- Secure data in transit between an application and Azure by using client-side encryption, HTTPS, or SMB 3.0.
- Set data to be automatically encrypted when it's written to Azure Storage by using storage service encryption.
- Grant delegated access to the data objects in Azure Storage by using shared access signatures.
- Use analytics to track the authentication method that someone is using when they access storage in Azure.

These security features apply to Azure Blob storage (block and page) and to Azure Files. Get detailed storage security guidance in the [Azure Storage security guide](#).

[Storage service encryption](#) provides encryption at rest and safeguards your data to meet your organization's security and compliance commitments. Storage service encryption is enabled by default for all managed disks, snapshots, and images in all the Azure regions. Starting June 10, 2017, all new managed disks, snapshots, images, and new data written to existing managed disks are automatically encrypted at rest with keys managed by Microsoft. For more information, see the [FAQ for managed disks](#).

Azure Disk Encryption allows you to encrypt managed disks that are attached to IaaS VMs as OS and data disks at rest and in transit by using your keys stored in [Azure Key Vault](#). For Windows, the drives are encrypted by using industry-standard [BitLocker](#) encryption technology. For Linux, the disks are encrypted by using the [dm-crypt](#) subsystem. The encryption process is integrated with Azure Key Vault to allow you to control and manage the disk encryption keys. For more information, see [Azure Disk Encryption for Windows and Linux IaaS VMs](#).

## Regional availability

You can use Azure to deliver services at the scale that you need to reach your customers and partners **wherever they are**. The [managed disks](#) and [Azure Storage](#) regional availability pages show the regions where these services are available. Checking the regional availability of a service beforehand can help you make the right decision for your workload and customer needs.

Managed disks are available in all Azure regions that have premium SSD and standard SSD offerings. Although ultra SSD currently is in public preview, it's offered in only one availability zone, the [East US 2](#) region. Verify the regional availability when you plan mission-critical, top-tier workloads that require ultra SSD.

Hot and cool Blob storage, Data Lake Storage Gen2, and Azure Files storage are available in all Azure regions. Archival blob storage, premium file shares, and premium block Blob storage are limited to certain regions. We recommend that you refer to the regions page to check the latest status of regional availability.

To learn more about Azure global infrastructure, see the [Azure regions page](#). You can also consult the [products available by region](#) page for specific details about what's available in each Azure region.

## Data residency and compliance requirements

Legal and contractual requirements that are related to data storage often will apply to your workloads. These requirements might vary based on the location of your organization, the jurisdiction of the physical assets that host your data stores, and your applicable business sector. Components of data obligations to consider include data classification, data location, and the respective responsibilities for data protection under the shared responsibility model. For help with understanding these requirements, see the white paper [achieving compliant data residency and security with Azure](#).

Part of your compliance efforts might include controlling where your database resources are physically located. Azure regions are organized into groups called geographies. An [Azure geography](#) ensures that data residency, sovereignty, compliance, and resiliency requirements are honored within geographical and political boundaries. If your workloads are subject to data sovereignty or other compliance requirements, you must deploy your storage resources to regions that are in a compliant Azure geography.

# Review your data options

11/9/2020 • 6 minutes to read • [Edit Online](#)

When you prepare your landing zone environment for your cloud adoption, you need to determine the data requirements for hosting your workloads. Azure database products and services support a wide variety of data storage scenarios and capabilities. How you configure your landing zone environment to support your data requirements depends on your workload governance, technical, and business requirements.

## Identify data services requirements

As part of your landing zone evaluation and preparation, you need to identify the data stores that your landing zone needs to support. The process involves assessing each of the applications and services that make up your workloads to determine their data storage and access requirements. After you identify and document these requirements, you can create policies for your landing zone to control allowed resource types based on your workload needs.

For each application or service you'll deploy to your landing zone environment, use the following decision tree as a starting point to help you determine the appropriate data store services to use:

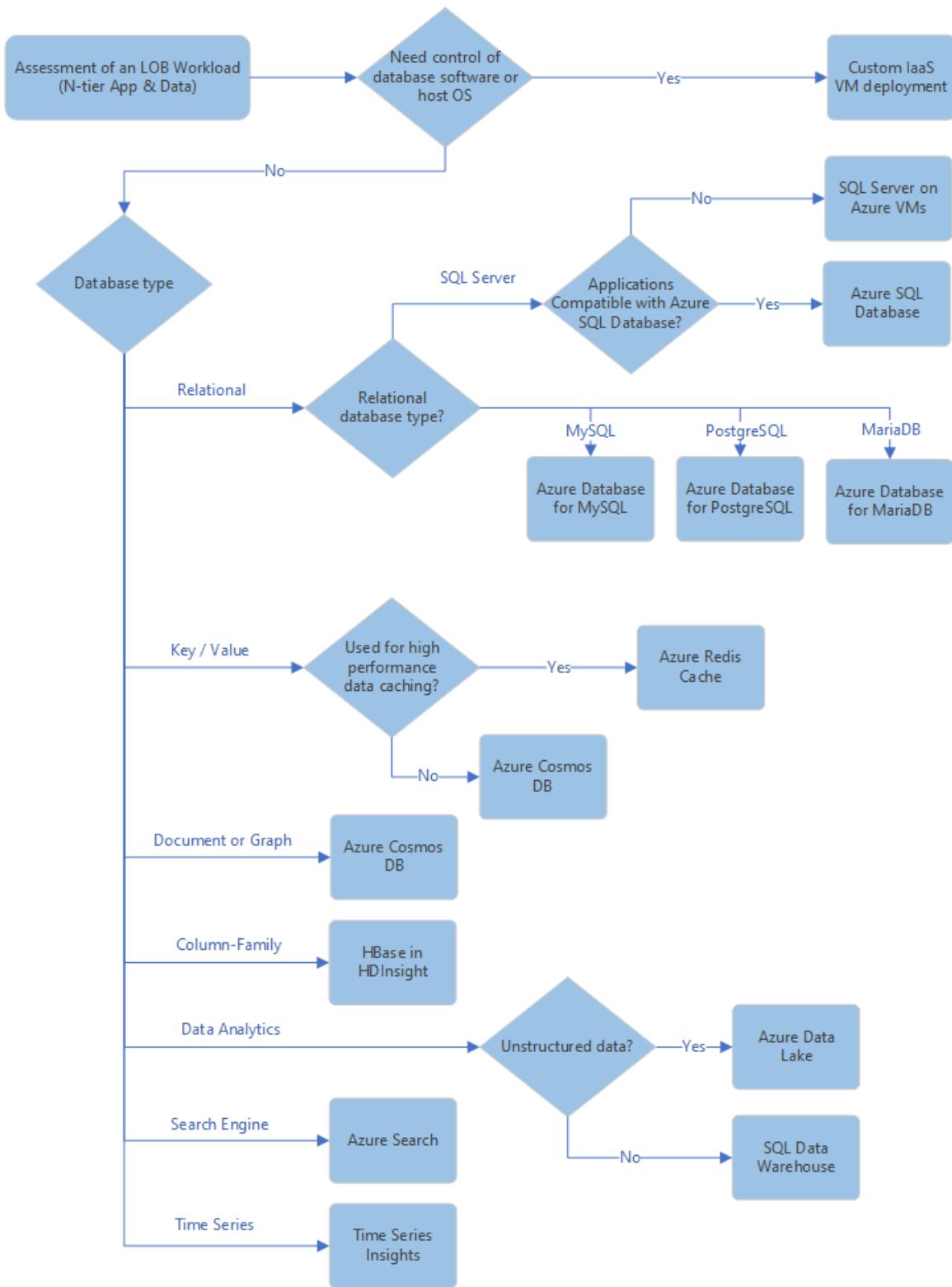


Figure 1:

An Azure database services decision tree.

## Key questions

Answer the following questions about your workloads to help you make decisions based on the Azure database services decision tree:

- **Do you need full control or ownership of your database software or host OS?** Some scenarios require you to have a high degree of control or ownership of the software configuration and host servers for your database workloads. In these scenarios, you can deploy custom infrastructure as a service (IaaS) virtual machines to fully control the deployment and configuration of data services. If you don't have these requirements, platform as a service (PaaS) database services might reduce your management and operations costs.
- **Will your workloads use a relational database technology?** If so, what technology do you plan to use?

Azure provides managed PaaS database capabilities for [Azure SQL Database](#), [MySQL](#), [PostgreSQL](#), and [MariaDB](#).

- **Will your workloads use SQL Server?** In Azure, you can have your workloads running in IaaS-based [SQL Server on Azure Virtual Machines](#) or on the PaaS-based [Azure SQL Database hosted service](#). Choosing which option to use is primarily a question of whether you want to manage your database, apply patches, and take backups, or if you want to delegate these operations to Azure. In some scenarios, compatibility issues might require the use of IaaS-hosted SQL Server. For more information about how to choose the correct option for your workloads, see [Choose the right SQL Server option in Azure](#).
- **Will your workloads use key/value database storage?** [Azure Cache for Redis](#) offers a high-performance cached key/value data storage solution that can power fast, scalable applications. [Azure Cosmos DB](#) also provides general-purpose key/value storage capabilities.
- **Will your workloads use document or graph data?** [Azure Cosmos DB](#) is a multi-model database service that supports a wide variety of data types and APIs. Azure Cosmos DB also provides document and graph database capabilities.
- **Will your workloads use column-family data?** [Apache HBase in Azure HDInsight](#) is built on Apache Hadoop. It supports large amounts of unstructured and semi-structured data in a schemaless database that's organized by column families.
- **Will your workloads require high-capacity data analytics capabilities?** You can use [Azure SQL Data Warehouse](#) to effectively store and query structured petabyte-scale data. For unstructured big data workloads, you can use [Azure data lake](#) to store and analyze petabyte-size files and trillions of objects.
- **Will your workloads require search engine capabilities?** You can use [Azure search](#) to build AI-enhanced cloud-based search indexes that can be integrated into your applications.
- **Will your workloads use time series data?** [Azure time series insights](#) is built to store, visualize, and query large amounts of time series data, such as data generated by IoT devices.

**NOTE**

Learn more about how to assess database options for each of your application or services in the [Azure application architecture guide](#).

## Common database scenarios

The following table illustrates a few common use scenario requirements and the recommended database services for handling them:

SCENARIO	DATA SERVICE
I need a globally distributed, multi-model database with support for NoSQL choices.	<a href="#">Azure Cosmos DB</a>
I need a fully managed relational database that provisions quickly, scales on the fly, and includes built-in intelligence and security.	<a href="#">Azure SQL Database</a>
I need a fully managed, scalable MySQL relational database that has high availability and security built in at no extra cost.	<a href="#">Azure Database for MySQL</a>
I need a fully managed, scalable PostgreSQL relational database that has high availability and security built in at no extra cost.	<a href="#">Azure Database for PostgreSQL</a>
I plan to host enterprise SQL Server apps in the cloud and have full control over the server OS.	<a href="#">SQL Server on virtual machines</a>

SCENARIO	DATA SERVICE
I need a fully managed elastic data warehouse that has security at every level of scale at no extra cost.	Azure SQL Data Warehouse
I need Data Lake Storage resources that are capable of supporting Hadoop clusters or HDFS data.	Azure data lake
I need high throughput and consistent, low-latency access for my data to support fast, scalable applications.	Azure Cache for Redis
I need a fully managed, scalable MariaDB relational database that has high availability and security built in at no extra cost.	Azure Database for MariaDB

## Regional availability

Azure lets you deliver services at the scale you need to reach your customers and partners, **wherever they are**. A key factor in planning your cloud deployment is to determine what Azure region will host your workload resources.

Most database services are generally available in most Azure regions. But there are a few regions, mostly targeting governmental customers, that support only a subset of these products. Before you decide which regions you will deploy your database resources to, we recommend that you refer to the [regions page](#) to check the latest status of regional availability.

To learn more about Azure global infrastructure, see the [Azure regions page](#). You can also view [products available by region](#) for specific details about the overall services that are available in each Azure region.

## Data residency and compliance requirements

Legal and contractual requirements that are related to data storage often will apply to your workloads. These requirements might vary based on the location of your organization, the jurisdiction of the physical assets that host your data stores, and your applicable business sector. Components of data obligations to consider include data classification, data location, and the respective responsibilities for data protection under the shared responsibility model. For help with understanding these requirements, see the white paper [achieving compliant data residency and security with Azure](#).

Part of your compliance efforts might include controlling where your database resources are physically located. Azure regions are organized into groups called geographies. An [Azure geography](#) ensures that data residency, sovereignty, compliance, and resiliency requirements are honored within geographical and political boundaries. If your workloads are subject to data sovereignty or other compliance requirements, you must deploy your storage resources to regions in a compliant Azure geography.

## Establish controls for database services

When you prepare your landing zone environment, you can establish controls that limit what data stores users can deploy. Controls can help you manage costs and limit security risks while still allowing developers and IT teams to deploy and configure resources that are needed to support your workloads.

After you identify and document your landing zone's requirements, you can use [Azure Policy](#) to control the database resources that you allow users to create. Controls can take the form of [allowing or denying the creation of database resource types](#). For example, you might restrict users to creating only Azure SQL Database resources. You can also use policy to control the allowable options when a resource is created, like [restricting what SQL Database SKUs can be provisioned](#) or [allowing only specific versions of SQL Server](#) to be installed on an IaaS VM.

Policies can be scoped to resources, resource groups, subscriptions, and management groups. You can include your

policies in [Azure blueprint](#) definitions and apply them repeatedly throughout your cloud estate.

# Role-based access control

11/9/2020 • 5 minutes to read • [Edit Online](#)

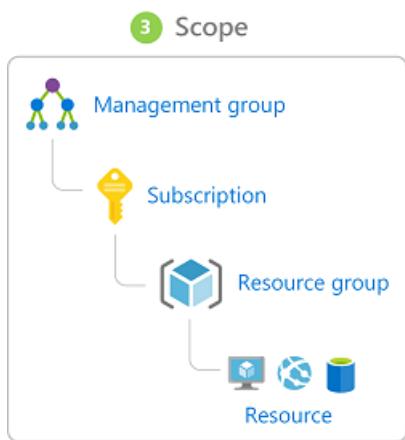
Group-based access rights and privileges are a good practice. Dealing with groups rather than individual users simplifies maintenance of access policies, provides consistent access management across teams, and reduces configuration errors. Assigning users to and removing users from appropriate groups helps keep current the privileges of a specific user. Azure [role-based access control \(RBAC\)](#) offers fine-grained access management for resources organized around user roles.

For an overview of recommended RBAC practices as part of an identity and security strategy, see [Azure identity management and access control security best practices](#).

## Overview of role-based access control

By using [role-based access control](#), you can separate duties within your team and grant only enough access for specific Azure Active Directory (Azure AD) users, groups, service principals, or managed identities to perform their jobs. Instead of giving everybody unrestricted access to your Azure subscription or resources, you can limit permissions for each set of resources.

[RBAC role definitions](#) list operations that are permitted or disallowed for users or groups assigned to that role. A role's [scope](#) specifies which resources these defined permissions apply to. Scopes can be specified at multiple levels: management group, subscription, resource group, or resource. Scopes are structured in a parent/child relationship.



For detailed instructions for assigning users and groups to specific roles and assigning roles to scopes, see [Manage access to Azure resources using RBAC](#).

When planning your access control strategy, use a least-privilege access model that grants users only the permissions required to perform their work. The following diagram shows a suggested pattern for using RBAC through this approach.

		Role		
Scope	Reader	Resource-specific or custom role	Contributor	Owner
Subscription	Observers	Users managing resources		Admins
Resource group				
Resource		Automated processes		

#### NOTE

The more specific or detailed permissions are that you define, the more likely it is that your access controls will become complex and difficult to manage. This is especially true as your cloud estate grows in size. Avoid resource-specific permissions. Instead, use [management groups](#) for enterprise-wide access control and [resource groups](#) for access control within subscriptions. Also avoid user-specific permissions. Instead, assign access to [groups in Azure AD](#).

## Use built-in RBAC roles

Azure provides a many built-in role definitions, with three core roles for providing access:

- The [Owner](#) role can manage everything, including access to resources.
- The [Contributor](#) role can manage everything except access to resources.
- The [Reader](#) role can view everything but not make any changes.

Beginning from these core access levels, additional built-in roles provide more detailed controls for accessing specific resource types or Azure features. For example, you can manage access to virtual machines by using the following built-in roles:

- The [virtual machine administrator login](#) role can view virtual machines in the portal and sign in as [administrator](#).
- The [virtual machine Contributor](#) role can manage virtual machines, but it can't access them or the virtual network or storage account they're connected to.
- The [virtual machine user login](#) role can view virtual machines in the portal and sign in as a regular user.

For another example of using built-in roles to manage access to particular features, see the discussion on controlling access to cost-tracking features in [Track costs across business units, environments, or projects](#).

For a complete list of available built-in roles, see [Built-in roles for Azure resources](#).

## Use custom roles

Although the roles built in to Azure support a wide variety of access control scenarios, they might not meet all the needs of your organization or team. For example, if you have a single group of users responsible for managing virtual machines and Azure SQL Database resources, you might want to create a custom role to optimize management of the required access controls.

The Azure RBAC documentation contains instructions on [creating custom roles](#), along with details on [how role definitions work](#).

## Separation of responsibilities and roles for large organizations

RBAC allows organizations to assign different teams to various management tasks within large cloud estates. It can allow Central IT teams to control core access and security features, while also giving software developers and other teams large amounts of control over specific workloads or groups of resources.

Most cloud environments can also benefit from an access-control strategy that uses multiple roles and emphasizes a separation of responsibilities between these roles. This approach requires that any significant change to resources or infrastructure involves multiple roles to complete, ensuring that more than one person must review and approve a change. This separation of responsibilities limits the ability of a single person to access sensitive data or introduce vulnerabilities without the knowledge of other team members.

The following table illustrates a common pattern for dividing IT responsibilities into separate custom roles:

GROUP	COMMON ROLE NAME	RESPONSIBILITIES
Security operations	SecOps	<p>Provides general security oversight. Establishes and enforces security policy such as encryption at rest.</p> <p>Manages encryption keys.</p> <p>Manages firewall rules.</p>
Network operations	NetOps	Manages network configuration and operations within virtual networks, such as routes and peerings.
Systems operations	SysOps	Specifies compute and storage infrastructure options, and maintains resources that have been deployed.
Development, test, and operations	DevOps	<p>Builds and deploys workload features and applications.</p> <p>Operates features and applications to meet service-level agreements and other quality standards.</p>

The breakdown of actions and permissions in these standard roles are often the same across your applications, subscriptions, or entire cloud estate, even if these roles are performed by different people at different levels. Accordingly, you can create a common set of RBAC role definitions to apply across different scopes within your environment. Users and groups can then be assigned a common role, but only for the scope of resources, resource groups, subscriptions, or management groups that they're responsible for managing.

For example, in a [hub and spoke network topology](#) with multiple subscriptions, you might have a common set of role definitions for the hub and all workload spokes. A hub subscription's NetOps role can be assigned to members of the organization's Central IT team, who are responsible for maintaining networking for shared services used by all workloads. A workload spoke subscription's NetOps role can then be assigned to members of that specific workload team, allowing them to configure networking within that subscription to best support their workload requirements. The same role definition is used for both, but scope-based assignments ensure that users have only the access that they need to perform their job.

# Create hybrid cloud consistency

11/9/2020 • 6 minutes to read • [Edit Online](#)

This article guides you through the high-level approaches for creating hybrid cloud consistency.

Hybrid deployment models during migration can reduce risk and contribute to a smooth infrastructure transition. Cloud platforms offer the greatest level of flexibility when it comes to business processes. Many organizations are hesitant to make the move to the cloud. Instead, they prefer to keep full control over their most sensitive data. Unfortunately, on-premises servers don't allow for the same rate of innovation as the cloud. A hybrid cloud solution offers the speed of cloud innovation and the control of on-premises management.

## Integrate hybrid cloud consistency

Using a hybrid cloud solution allows organizations to scale computing resources. It also eliminates the need to make massive capital expenditures to handle short-term spikes in demand. Changes to your business can drive the need to free up local resources for more sensitive data or applications. It's easier, faster, and less expensive to deprovision cloud resources. You pay only for those resources your organization temporarily uses, instead of having to purchase and maintain additional resources. This approach reduces the amount of equipment that might remain idle over long periods of time. Hybrid cloud computing delivers all the benefits of cloud computing flexibility, scalability, and cost efficiencies with the lowest possible risk of data exposure.

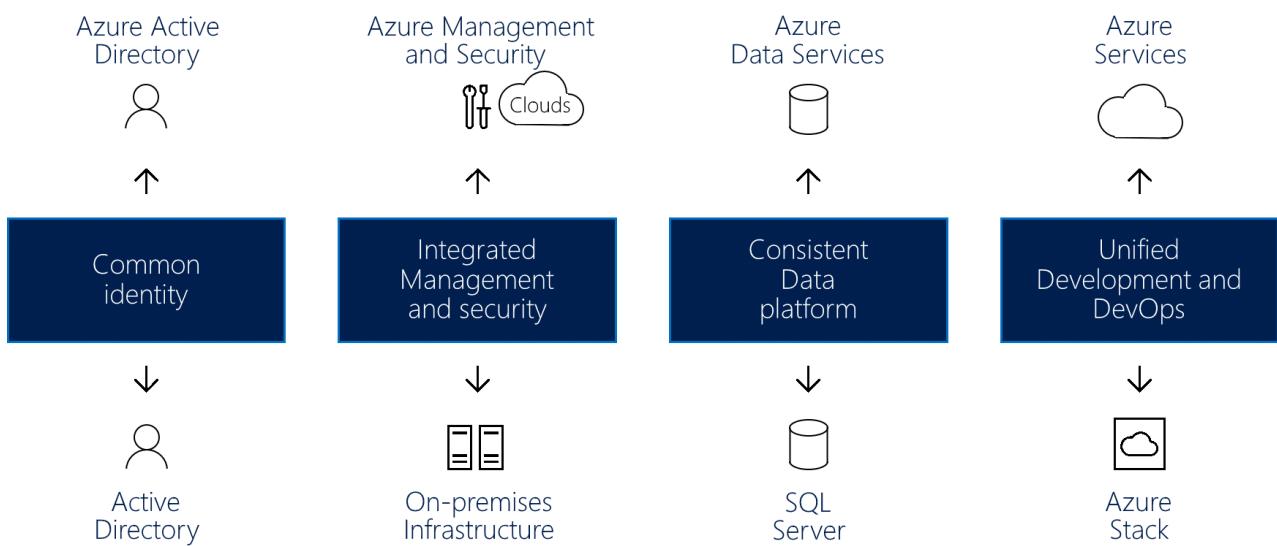


Figure 1: Creating hybrid cloud consistency across identity, management, security, data, development, and DevOps.

A true hybrid cloud solution must provide four components, each of which brings significant benefits:

- **Common identity for on-premises and cloud applications:** This component improves user productivity by giving users single sign-on (SSO) to all their applications. It also ensures consistency as applications and users cross network or cloud boundaries.
- **Integrated management and security across your hybrid cloud:** This component provides you with a cohesive way to monitor, manage, and secure the environment, which enables increased visibility and control.
- **A consistent data platform for the datacenter and the cloud:** This component creates data portability, combined with seamless access to on-premises and cloud data services for deep insight into all data sources.
- **Unified development and DevOps across the cloud and on-premises datacenters:** This component allows you to move applications between the two environments as needed. Developer productivity improves because both locations now have the same development environment.

Here are some examples of these components from an Azure perspective:

- Azure Active Directory (Azure AD) works with on-premises Active Directory to provide common identity for all users. SSO across on-premises and via the cloud makes it simple for users to safely access the applications and assets they need. Admins can manage security and governance controls and also have the flexibility to adjust permissions without affecting the user experience.
- Azure provides integrated management and security services for both cloud and on-premises infrastructure. These services include an integrated set of tools that are used to monitor, configure, and protect hybrid clouds. This end-to-end approach to management specifically addresses real-world challenges that face organizations considering a hybrid cloud solution.
- Azure hybrid cloud provides common tools that ensure secure access to all data, seamlessly and efficiently. Azure data services combine with Microsoft SQL Server to create a consistent data platform. A consistent hybrid cloud model allows users to work with both operational and analytical data. The same services are provided on-premises and in the cloud for data warehousing, data analysis, and data visualization.
- Azure cloud services, combined with Azure Stack on-premises, provide unified development and DevOps. Consistency across the cloud and on-premises means that your DevOps team can build applications that run in either environment and can easily deploy to the right location. You also can reuse templates across the hybrid solution, which can further simplify DevOps processes.

## Azure Stack in a hybrid cloud environment

Azure Stack is a hybrid cloud solution that allows organizations to run Azure-consistent services in their datacenter. It provides a simplified development, management, and security experience that's consistent with Azure public cloud services. Azure Stack is an extension of Azure. You can use it to run Azure services from your on-premises environments and then move to the Azure cloud if and when required.

With Azure Stack, you can deploy and operate both IaaS and PaaS by using the same tools and offering the same experience as the Azure public cloud. Management of Azure Stack, whether through the web ui portal or through PowerShell, has a consistent look and feel for IT administrators and end users with Azure.

Azure and Azure Stack open up new hybrid use cases for both customer-facing and internal line-of-business applications:

- **Edge and disconnected solutions.** To address latency and connectivity requirements, customers can process data locally in Azure Stack and then aggregate it in Azure for further analytics. They can use common application logic across both. Many customers are interested in this edge scenario across different contexts, like factory floors, cruise ships, and mine shafts.
- **Cloud applications that meet various regulations.** Customers can develop and deploy applications in Azure, with full flexibility to deploy on-premises on Azure Stack to meet regulatory or policy requirements. No code changes are needed. Application examples include global audit, financial reporting, foreign exchange trading, online gaming, and expense reporting. Customers sometimes look to deploy different instances of the same application to Azure or Azure Stack, based on business and technical requirements. While Azure meets most requirements, Azure Stack complements the deployment approach where needed.
- **Cloud application model on-premises.** Customers can use Azure web services, containers, microservices, and serverless architectures to update and extend existing applications or build new ones. You can use consistent DevOps processes across Azure in the cloud and Azure Stack on-premises. There's a growing interest in application modernization, even for core mission-critical applications.

Azure Stack is offered via two deployment options:

- **Azure Stack integrated systems:** Azure Stack integrated systems are offered through Microsoft and hardware partners to create a solution that provides cloud-paced innovation balanced with simple management. Because Azure Stack is offered as an integrated system of hardware and software, you get flexibility and control while still adopting innovation from the cloud. Azure Stack integrated systems range in

size from 4 to 12 nodes. They're jointly supported by the hardware partner and Microsoft. Use Azure Stack integrated systems to enable new scenarios for your production workloads.

- **Azure Stack Development Kit:** The Microsoft Azure Stack Development Kit is a single-node deployment of Azure Stack. You can use it to evaluate and learn about Azure Stack. You can also use the kit as a developer environment, where you can develop by using APIs and tooling that are consistent with Azure. The Azure Stack Development Kit isn't intended for use as a production environment.

## Azure Stack one-cloud ecosystem

You can speed up Azure Stack initiatives by using the complete Azure ecosystem:

- Azure ensures that most applications and services that are certified for Azure will work on Azure Stack. Several ISVs are extending their solutions to Azure Stack. These ISVs include Bitnami, Docker, kemp technologies, pivotal cloud foundry, Red Hat enterprise Linux, and suse Linux.
- You can opt to have Azure Stack delivered and operated as a fully managed service. Several partners will have managed service offerings across Azure and Azure Stack shortly. These partners include tieto, Yourhosting, Revera, Pulsant, and ntt. These partners deliver managed services for Azure via the Cloud Solution Provider (CSP) program. They're extending their offerings to include hybrid solutions.
- As an example of a complete, fully managed hybrid cloud solution, Avanade delivers an all-in-one offer. It includes cloud transformation services, software, infrastructure, setup and configuration, and ongoing managed services. This way customers can consume Azure Stack just as they do with Azure today.
- Providers can help accelerate application modernization initiatives by building end-to-end Azure solutions for customers. Each provider brings a deep Azure skill set, domain and industry knowledge, and process expertise such as DevOps. Every Azure Stack implementation is an opportunity for a provider to design the solution and lead and influence system deployment. They can also customize the included capabilities and deliver operational activities. Examples of providers include Avanade, DXC, Dell EMC Services, Infront Consulting Group, HPE Pointnext, and PWC (formerly PricewaterhouseCoopers).

# Improve landing zone operations

11/9/2020 • 2 minutes to read • [Edit Online](#)

Landing zone operations provide the initial foundation for operations management. As operations scale, these improvements will refactor landing zones to meet growing operational excellence, reliability, and performance requirements.

## Landing zone operations best practices

The following links provide best practices for improving landing zone operations.

- [Azure server management](#): An onboarding guide to incorporating the cloud-native tools and services needed to manage operations.
- [Hybrid monitoring](#): Many customers have already made a substantial investment in System Center Operations Manager. For those customers, this guide to hybrid monitoring can help them compare and contrast the cloud-native reporting tools with Operations Manager tooling. This comparison makes it easier to decide which tools to use for operational management.
- [Centralize management operations](#): Use Azure Lighthouse to centralize operations management across multiple Azure tenants.
- [Establish an operational fitness review](#): Review an environment for operational fitness.
- Workload specific operations best practices:
  - [Resiliency checklist](#)
  - [Failure mode analysis](#)
  - [Recover from a region wide service disruption](#)
  - [Recover from data corruption or accidental deletion](#)

## Four steps to improve operations beyond a single landing zone

The [Manage methodology](#) provides overall guidance for building out operations management capacity, see the [Manage methodology](#). We will use the basic structure of that methodology and the following steps from that methodology to improve landing zone operations and operations across all landing zones.

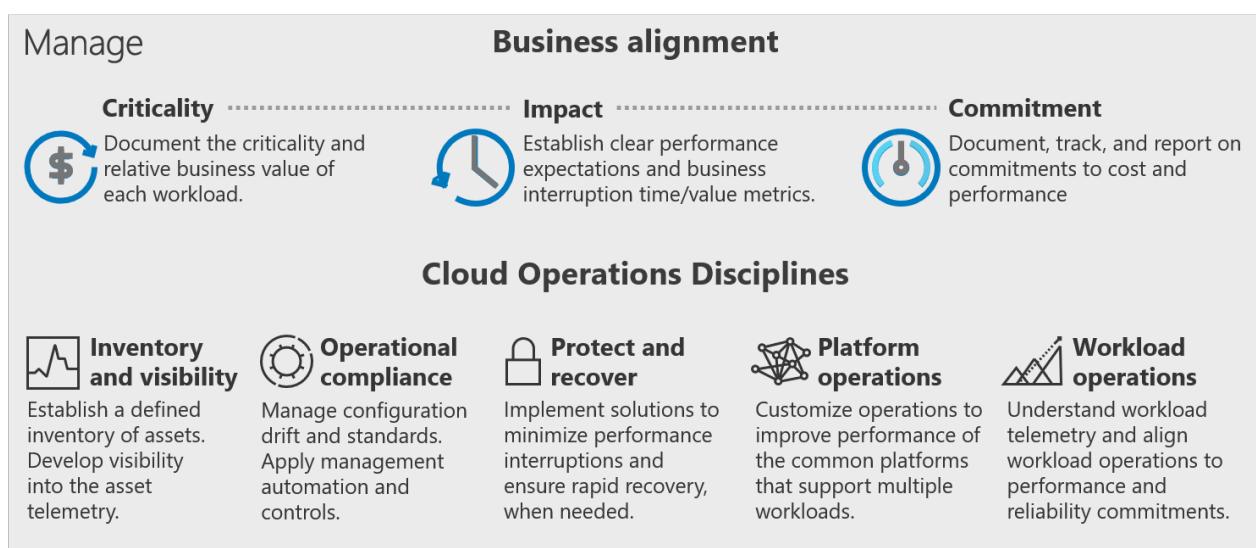


Figure 1: The Manage methodology of the Cloud Adoption Framework.

1. [Establish a management baseline](#): A management baseline establishes the foundation for operations

management. The guidance under this first step can be applied to any landing zone to improve initial operations.

2. **Define business commitments:** Understanding the criticality and impact of each workload within a landing zone will establish a "definition of done" for any ongoing management improvements for any landing zone. This process will also identify the reliability, performance, and operations requirements of each workload.
3. **Expand the management baseline:** This set of best practices can be applied to improve landing zone operations beyond the initial baseline.
4. **Advanced operations and design principles:** Review the design and operations of specific workloads, platforms, or full landing zones to meet deeper requirements.

## Test-driven development cycle

Before beginning any security improvements, it's important to understand the "definition of done" and all "acceptance criteria". For more information, see the articles on [test-driven development of landing zones](#) and [test-driven development in Azure](#).

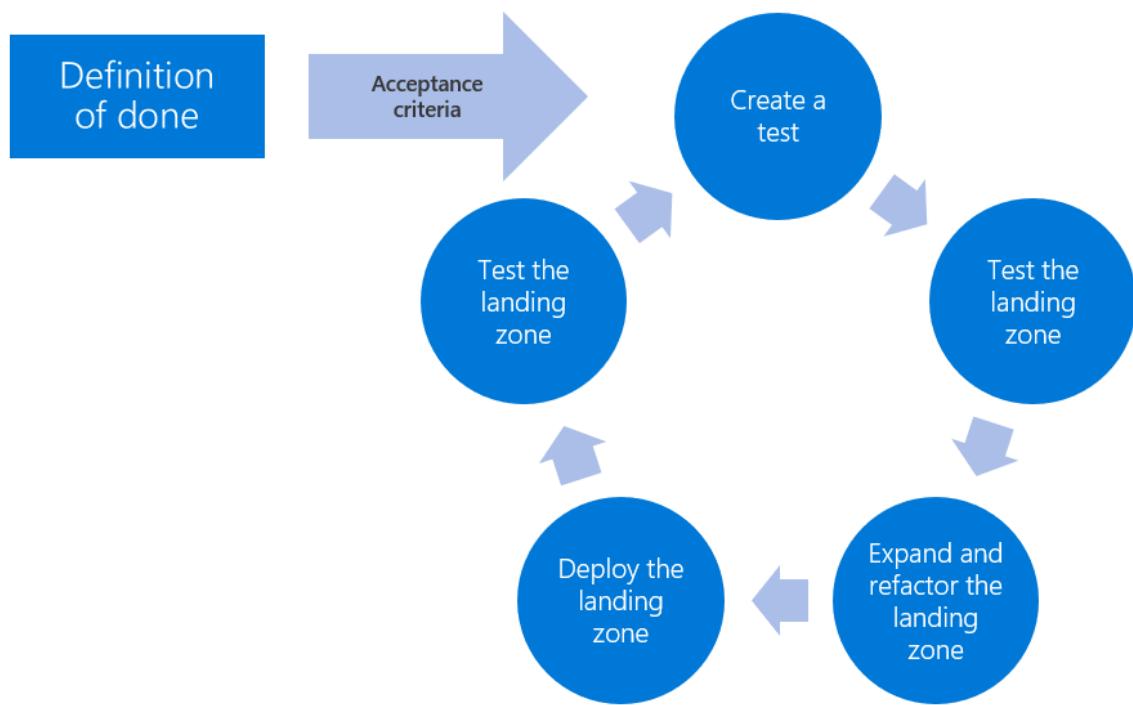


Figure 2: The test-driven development process for cloud landing zones.

## Next steps

Understand how to [improve landing zone governance](#) to support adoption at scale.

[Improve landing zone governance](#)

# Improve landing zone governance

11/9/2020 • 2 minutes to read • [Edit Online](#)

Landing zone governance is the smallest unit of overall governance. Establishing a sound governance foundation within your first few landing zones will reduce the amount of refactoring required later in the adoption lifecycle. Improving landing zone governance will integrate cost controls, establish basic tooling to allow for scale, and will make it easier for the cloud governance team to deliver on the Five Disciplines of Cloud Governance.

## Landing zone governance best practices

- **Initial landing governance:** The article on establishing an [initial governance foundation](#) can assist with adding initial governance tooling to the first few landing zones. These practices will aid in scaling adoption and governance, along with implementing sound cost management. This approach starts with: resource organization, policy definitions, RBAC roles, and blueprint definitions.
- **Naming and tagging standards:** Ensure consistency in naming and tagging, which is the foundational data for establishing sound governance practices.
- **Track costs across workloads:** Begin tracking costs in your first landing zone. Evaluate how you will apply consistency across multiple workloads and roles.
- **Scale with multiple subscriptions:** Evaluate how this landing zone and other landing zones will scale, as multiple subscriptions become a requirement.
- **Organize subscriptions:** Understand how to organize and manage multiple subscriptions.

## Four steps to improve overall governance

The [Govern methodology](#) provides overall guidance for building out governance policies, processes, and disciplines. We will use the basic structure of that methodology and the following steps from that methodology to improve landing zone governance and governance across all landing zones.

1. [Understand the methodology:](#) Understand the basic methodology to guide end-state governance design.
2. [Benchmark:](#) Assess both current and future state to establish a vision and take action.
3. [Initial governance foundation:](#) Small, easily implemented set of governance tools to establish an initial foundation for all landing zones.
4. [Improve the governance foundation:](#) Iteratively add governance controls to strengthen all landing zone governance.

## Next steps

Cloud adoption will continue to expand with each wave or release of new workloads. To stay ahead of these requirements, cloud platform teams should periodically review additional landing zone best practices.

[Review additional landing zone best practices](#)

# Improve landing zone security

11/9/2020 • 2 minutes to read • [Edit Online](#)

When a workload or the landing zones that hosts it require access to any sensitive data or critical systems, it's important to protect the data and assets. Improving landing zone security builds on the [test-driven development approach to landing zones](#) by expanding or refactoring the landing zone to account for heightened security requirements.

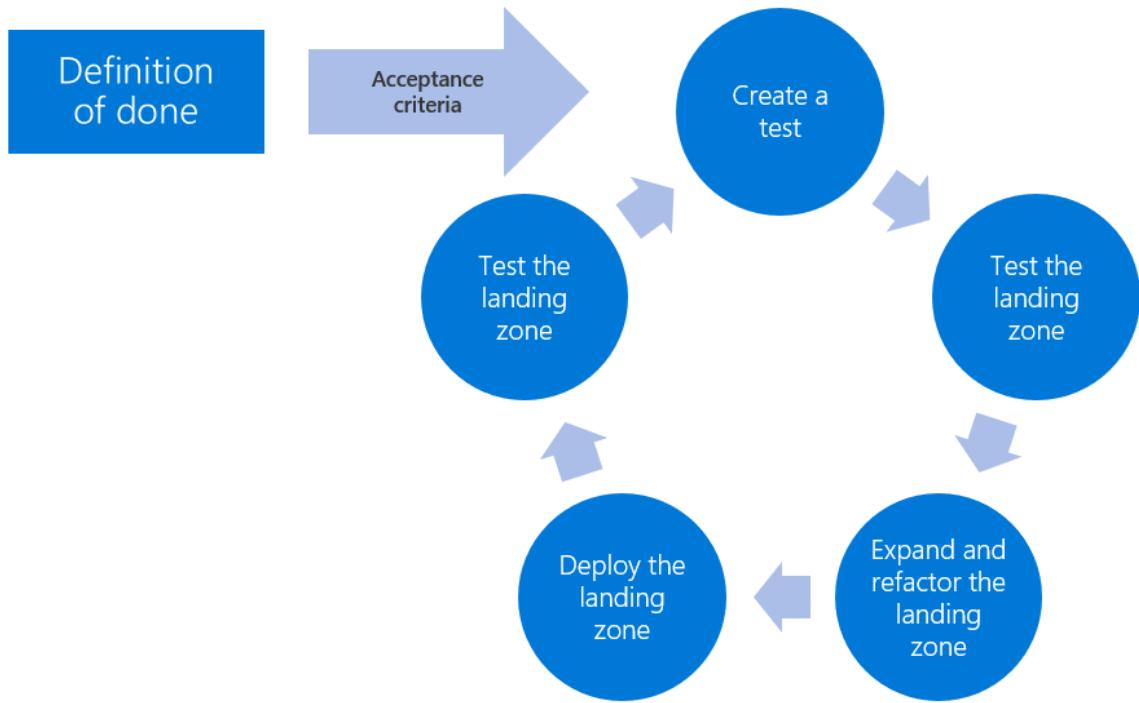
## Landing zone security best practices

The following list of reference architectures and best practices provides examples of ways to improve landing security:

- [Azure Security Center](#): Onboard a subscription to Security Center.
- [Azure Sentinel](#): Onboard Azure Sentinel to provide a **security information event management (SIEM)** and **security orchestration automated response (SOAR)** solution.
- [Network boundary security](#): Several reference patterns for developing a network, similar to how the network boundary is secured in a datacenter.
- [Secure network architecture](#): Reference architecture for implementing a perimeter network and secure network architecture.
- [Identity management and access control](#): Series of best practices for implementing identity and access to secure a landing zone in Azure.
- [Network security practices](#): Provides additional best practices for securing the network.
- [Operational security](#) provides best practices for increasing operational security in Azure.
- The [Security Baseline discipline](#): Example of developing a governance-driven security baseline to enforce security requirements.

## Test-driven development cycle

Before beginning any security improvements, it's important to understand the "definition of done" and all "acceptance criteria". For more information, see the articles on [test-driven development of landing zones](#) and [test-driven development in Azure](#).



## Next steps

Understand how to [improve landing zone operations](#) to support critical applications.

[Improve landing zone operations](#)

# Evaluate a Microsoft partner's Azure landing zone

11/9/2020 • 8 minutes to read • [Edit Online](#)

The Cloud Adoption Framework approaches cloud adoption as a self-service activity. The objective is to empower each team that supports adoption through standardized approaches. In practice, you can't assume that a self-service approach is sufficient for all adoption activities.

Successful cloud adoption programs typically involve at least one level of third-party support. Many cloud adoption efforts require support from a systems integrator (SI) or consulting partner who provides services that accelerate cloud adoption. Managed service providers (MSPs) provide enduring value by supporting landing zones and cloud adoption, but they also provide post-adoption operations management support. Additionally, successful cloud adoption efforts tend to engage one or more independent software vendors (ISV) who provide software-based services that accelerate cloud adoption. The rich partner ecosystems of SIs, ISVs, MSPs, and other forms of Microsoft partners have aligned their offerings to specific methodologies found in the Cloud Adoption Framework. When a partner is aligned to the Ready methodology of this framework, they will likely offer their own Azure landing zone implementation option.

This article provides a set of questions that help create an understanding of the scope of the partner's Azure landing zone implementation options.

## IMPORTANT

Partner offers and Azure landing zone implementation options are defined by the partner, based on their extensive experience helping customers adopt the cloud.

Partners might choose to omit the implementation of specific design areas in their initial landing zone implementation. However, they should be able to communicate when and how each design area is implemented, as well as a range of costs for completing that design area whenever possible.

Other partner solutions might be flexible enough to support multiple options for each of the questions below. Use these questions to ensure you're comparing partner offers and self-service options equally.

## Find a partner

If you need a partner to implement your Azure landing zones, start with the approved list of Cloud Adoption Framework aligned partners. Specifically, start with partners who have [offers aligned to the Ready methodology](#).

Additionally, all [Azure expert managed service providers \(MSPs\)](#) have been audited to validate their ability to deliver each methodology of the Cloud Adoption Framework. While a particular partner might not have an aligned offer, all partners have demonstrated alignment during technical delivery.

## Validate a partner offer

Once a partner is selected, use the remainder of this article to guide your validation of the partner offer. Each section includes a summary of what to look for and a list of questions to ask the partner. The partner's answers to these questions shouldn't be considered as right or wrong. Instead, the questions are designed to help you evaluate whether the partner offer will meet your business requirements.

## Platform development velocity

As outlined in the [Azure landing zone implementation options](#), there are two high-level approaches to landing

zone implementation based on how you want to develop your landing zones.

**Question for the partner:** Which of the following approaches are supported by the partner's Azure landing zone solution?

- **Start small and expand:** Begin with a lightweight template. The landing zone solution is matured over time as your desired cloud operating model becomes clearer.
- **Start with enterprise scale:** Begin with a more comprehensive reference implementation. The reference architecture builds on a well-defined cloud operating model that requires less iteration to reach a mature solution.
- **Other:** The partner has a modified approach and should be able to describe the approach.

## Design principles

All Azure landing zones must consider the following set of common design areas. We refer to the way those design areas are implemented as design principles. The following sections will help validate the partner's design principles that define the Azure landing zone implementation.

### Deployment options

Partners who offer an Azure landing zone solution might support one or more options to deploy (or modify/expand the landing zone) the solution to your Azure tenant.

**Question for the partner:** Which of the following does your Azure landing zone solution support?

- **Configuration automation:** Does the solution deploy the landing zone from a deployment pipeline or deployment tool?
- **Manual configuration:** Does the solution empower the IT team to manually configure the landing zone, without injecting errors into the landing zone source code?

**Question for the partner:** Which of the Azure landing zone implementation options are supported by the partner's solution? See the [Azure landing zone implementation options](#) article for a full list of options.

### Identity

Identity is perhaps the most important design area to evaluate in the partner solution.

**Question for the partner:** Which of the following identity management options does the partner solution support?

- **Azure AD:** The suggested best practice is to use Azure AD and role-based access control to manage identity and access in Azure.
- **Active Directory:** If required, does the partner solution provide an option to deploy Active Directory as an infrastructure as a service solution?
- **Third-party identity provider:** If your company uses a third-party identity solution, determine whether and how the partner's Azure landing zone integrates with the third-party solution.

### Network topology and connectivity

Networking is arguably the second most important design area to evaluate. There are several best practice approaches to network topology and connectivity.

**Question for the partner:** Which of the following options is included with the partner's Azure landing zone solution? Are any of the following options incompatible with the partner's solution?

- **Virtual network:** Does the partner solution configure a virtual network? Can its topology be modified to meet your technical or business constraints?
- **Virtual private network (VPN):** Is VPN configuration included in the partner's landing zone design to connect the cloud to existing datacenters or offices?

- **High-speed connectivity:** Is a high-speed connection such as Azure ExpressRoute included in the landing zone design?
- **Virtual network peering:** Does the design include connectivity between different subscriptions or virtual networks in Azure?

## Resource organization

Sound governance and operational management of the cloud starts with best practice resource organization.

**Question for the partner:** Does the partner's landing zone design include considerations for the following resource organization practices?

- **Naming standards:** What [naming standards](#) will this offering follow and is that standard automatically enforced through policy?
- **Tagging standards:** Does the landing zone configuration follow and enforce a specific [standards for tagging assets](#)?
- **Subscription design:** What [subscription design strategies](#) are supported by the partner offer?
- **Management group design:** Does the partner offer follow a defined pattern for the [Azure management group hierarchy](#) to organize subscriptions?
- **Resource group alignment:** How are resource groups used to group assets deployed to the cloud? In the partner offer, are resource groups used to group assets into workloads, deployment packages, or other organization standards?

**Question for the partner:** Does the partner provide onboarding documentation to [track foundational decisions](#) and educate staff? See the [initial decision template](#) for an example of such documentation.

## Governance disciplines

Your governance requirements can heavily influence any complex landing zone designs. Many partners provide a separate offering to fully implement governance disciplines after landing zones are deployed. The following questions will help create clarity around the aspects of governance that will be built into any landing zones.

**Question for the partner:** What governance tooling does the partner solution include as part of the landing zone implementation?

- **Policy compliance monitoring:** Does the partner's landing zone solution includes defined governance policies along with tools and processes to monitor compliance? Does the offer include customization of policies to fit your governance needs?
- **Policy enforcement:** Does the partner's landing zone solution include automated enforcement tools and processes?
- **Cloud platform governance:** Does the partner offer include a solution for maintaining compliance to a common set of policies across all subscriptions? Or is the scope limited to individual subscriptions?
- **N/A:** Start-small approaches intentionally postpone governance decisions until the team has deployed low-risk workloads to Azure. This can be addressed in a separate offer after the landing zone solution has been deployed.

**Question for the partner:** Does the partner offer go beyond governance tooling to also include processes and practices for delivering any of the following cloud governance disciplines?

- **Cost management:** Does the partner offer prepare the team to evaluate, monitor, and optimize spend while creating cost accountability with workload teams?
- **Security baseline:** Does the partner offer prepare the team to maintain compliance as security requirements change and mature?
- **Resource consistency:** Does the partner offer prepare the team to ensure that all assets in the cloud are onboarded into relevant operations management processes?
- **Identity baseline:** Does the partner offer prepare the team to maintain identity, role definitions, and

assignments after the initial landing zone is deployed?

### Operations baseline

Your operations management requirements could influence configuration of specific Azure products during landing zone implementation. Many partners provide a separate offering to fully implement the operations baseline and advanced operations later in the cloud adoption journey, but before your first workload is released for production use. But, the partner's landing zone solution might include configuration for a number of operations management tools by default.

**Question for the partner:** Does the partner solution include design options to support any of the cloud operations disciplines?

- **Inventory and visibility:** Does the landing zone include tooling to ensure that 100% of assets are centrally monitored?
- **Operational compliance:** Does the architecture include tooling and automated processes to enforce patching or other operational compliance requirements?
- **Protect and recover:** Does the partner offer include tooling and configuration to ensure a minimal standard of backup and recovery for 100% of assets deployed?
- **Platform operations:** Does the landing zone offering include tooling or processes to optimize operations across the portfolio?
- **Workload operations:** Does the landing zone offering include tooling to manage workload-specific operations requirements and ensure that each workload is well-architected?

## Take action

After reviewing the partner's Azure landing zone offer or solution using the questions above, your team will be better equipped to choose the partner whose Azure landing zone most closely aligns to your cloud operating model.

If you determine that a self-service approach to Azure landing zone deployment is a better fit, review or revisit the [Azure landing zone implementation options](#) to find the templated landing zone approach that best aligns with your cloud operating model.

## Next steps

Learn about the process for refactoring landing zones.

[Refactor landing zones](#)

# Refactor landing zones

11/9/2020 • 7 minutes to read • [Edit Online](#)

A landing zone is an environment for hosting your workloads that's **preprovisioned through code**. Since landing zone infrastructure is defined in code, it can be refactored similar to any other codebase. Refactoring is the process of modifying or restructuring source code to optimize the output of that code without changing its purpose or core function.

The Ready methodology uses the concept of refactoring to accelerate migration and remove common blockers. The steps in the ready overview discuss a process that starts with predefined landing zone template that aligns best with your hosting function. Then refactor or add to the source code to expand the landing zones ability to deliver that function through improved security, operations, or governance. The following image illustrates the concept of refactoring.

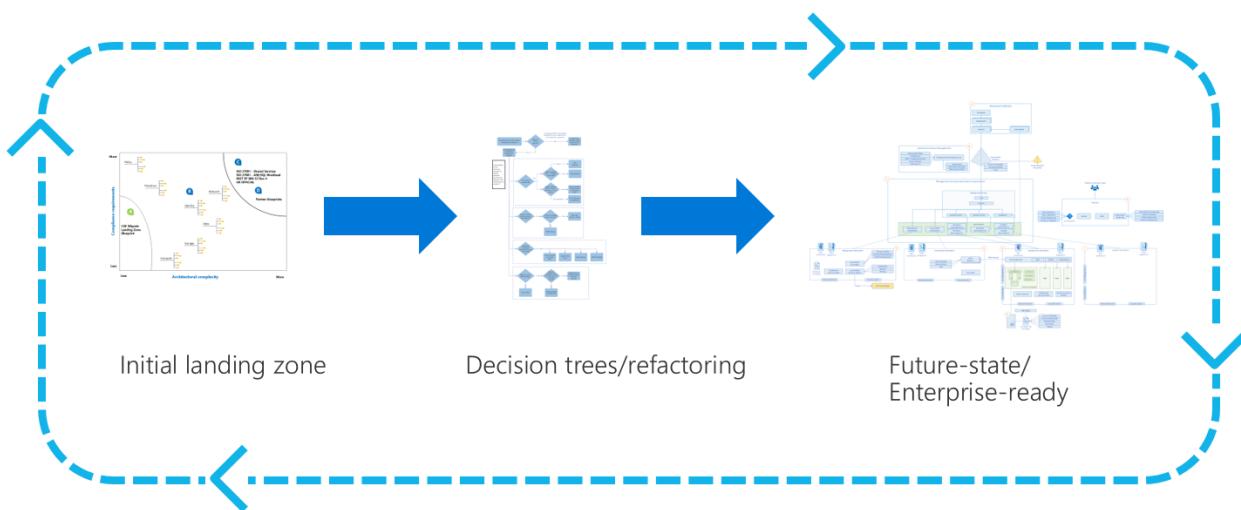


Figure 1: Landing zone refactoring.

## Common blockers

When customers adopt the cloud, landing zone considerations are the single most common blocker to adoption and cloud-related business results. Customers tend to lean towards one of the following two blockers. Various teams often lean towards one of these two blockers, resulting in cultural deadlocks that make adoption difficult.

Both of the primary blockers are rooted in one belief, the cloud environment and the existing datacenters should be at or near feature parity regarding operations, governance, and security. This is a wise long-term goal. But the pain comes from the delicate balance between the timing to achieve that goal and the speed required to deliver business results.

### Blocker: Acting too soon

It took years and significant effort to reach the current state of security, governance, and operations in the current datacenter. It also required observations, learning, and customization to meet the unique constraints of that environment. Replicating those same procedures and configurations will take time. Reaching complete feature parity may also result in an environment that underperforms in the cloud. This parity approach also commonly leads to significant unplanned overspending in the cloud environment. Don't try to apply current-state requirements to a future-state environment as an early stage gate. Such an approach rarely proves to be profitable.



*Figure 2: Acting too soon is a common blocker.*

In the image above, the customer has an objective of 100 workloads running in the cloud. To get there, the customer will likely deploy their first workload and then their first ten or so workloads before they're ready to release one of them to production. Eventually, they'll reach the objective of the adoption plan and have a robust portfolio in the cloud. But the red *x* in the image shows where customers commonly get stuck. Waiting for total alignment can delay the first workload by weeks, months, or even years.

## **Blocker: Acting too late**

On the other hand, acting too late can have significant long-term consequences on the success of the cloud adoption effort. If the team waits to reach feature parity until the adoption efforts are complete, they will encounter unnecessary roadblocks and require several escalations to keep the efforts on track.



*Figure 3: Acting too late is a common blocker.*

Similar to acting too soon, in this image, the customer waits too long to reach enterprise readiness across landing zones. By waiting too long, the customer will be constrained on the amount of refactoring and expansion they can do in the environment. Those constraints will limit their ability to drive continued success.

## Finding balance

To avoid these common blockers, we suggest an iterative approach based on well-structured cloud adoption plan, which maximizes learning opportunities and minimizes time to business success. Refactoring and parallel efforts are critical to this approach.

**WARNING**

Adoption teams who have a mid-term objective (within 24 months) to **host more than 1,000 assets (apps, infrastructure, or data assets) in the cloud** are highly unlikely to be successful using a refactoring approach. The learning curve is too high and the timeline too tight to allow for organic approaches to skills attainment. A more complete starting point requiring less customization will be a better path to achieve your objectives. Your implementation partners will likely be able to guide you through a better approach.

The remainder of this article will focus on some key constraints that can empower a refactoring approach, while minimizing risk.

## Theory

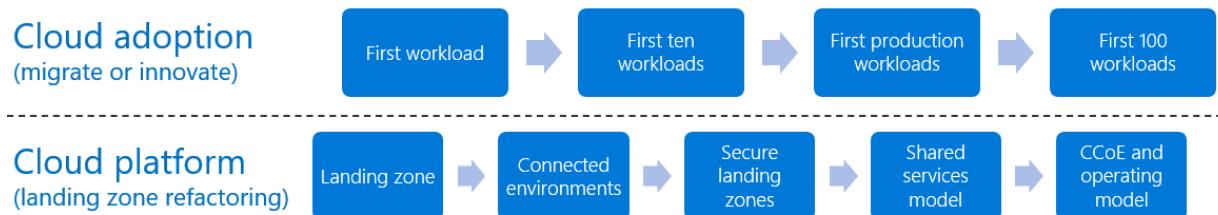
The concept of refactoring a landing zone is simple, but execution requires proper guardrails. The concept shown above outlines the basic flow:

- When you're ready to build your first landing zone, start with an initial landing zone defined via a template.

- Once that landing zone is deployed, use the decision trees in the subsequent articles under the [Expand your landing zone](#) section of the table of contents to refactor and add to your initial landing zone.
- Repeat decision trees and refactoring until you have an enterprise-ready environment that meets the enhanced requirements of your security, operations, and governance teams.

## Development approach

The advantage of a refactoring-based approach, is the ability to create parallel iteration paths for development. The image below provides an example of two parallel iteration paths: cloud adoption and cloud platform. Both progress at their own pace, with minimal risk of becoming a blocker to either team's daily efforts. Alignment on the adoption plan and refactoring guardrails can lead to agreement about milestones and clarity about future-state dependencies.



*Figure 4: Landing zone parallel iteration.*

In the example iteration paths above, the cloud adoption team is migrating their portfolio of 100 workloads to the cloud. In parallel, the cloud platform team is focused on staying ahead of the cloud adoption plan to ensure the environment is prepared for those workloads.

In this example, the planned iterations run as follows:

- The cloud platform team starts the development efforts by deploying an initial landing zone. That landing zone allows the cloud adoption team to deploy and begin testing their first workload.
- To prepare for the cloud adoption team's next deployment of 10 workloads, the cloud platform team works ahead to refactor and add a connected environment, treating the cloud as a perimeter network.
- Before the adoption team can release their first production workload, the security team requires a security review. While the adoption team deploys their first 10 workloads, the platform team moves ahead to define and implement security requirements.
- By the time the first workload is released to production, both teams should have enough learnings to prepare for a longer term shared service model. Centralizing core service architectures will help align governance and operations team. Centralizing core services will help prepare the adoption team to scale and release the next several waves of production workloads.
- As the team approaches their goal of migrating 100 workloads, the team will naturally begin to move towards more of a cloud center of excellence collaboration model and team structure.

Configuring an enterprise-ready environment will take time. This approach will not eliminate that requirement. Instead, this approach is designed to remove early blockers and create opportunities for the platform and adoption teams to learn together.

## Landing zone refactoring guardrails

All initial landing zone templates have limitations. Guardrails or policies during refactoring should reflect those limitations. Before beginning a landing zone refactoring process, it is important to understand the long-term requirements of the cloud adoption plan and classification of the candidate workloads, compared to the initial template limitations.

As an example of establishing refactoring guardrails, let's compare the development approach in the prior example

and the CAF Migration landing zone blueprint.

- Per the [assumptions of the CAF Migration landing zone blueprint](#), this initial landing zone is not designed for sensitive data or mission-critical workloads. Those features will have to be added through refactoring.
- In this example, let's assume that the portfolio of 100 workloads will require both mission critical and sensitive data hosting capabilities.

To balance these two competing requirements, the adoption team and platform team will agree to and operate under the following conditions:

- The cloud adoption team will prioritize production workloads that don't have access to sensitive data and are not deemed mission critical.
- Prior to production release, the security and operations team will validate alignment to the prior policy.
- The cloud platform team will work with the security and governance teams to implement a security baseline. Once security approves the implementation, the adoption team will be cleared to migrate workloads that have access to some sensitive data.
- The cloud platform team will work with the operations team to implement a management baseline. Once the operations team approves the implementation, the adoption team will be cleared to migrate workloads with a higher level of criticality.

For this example, the above set of agreed upon conditions will allow the adoption team get started on their migration effort. It also helps the platform team shape their interactions with other teams, as they build towards a longer-term enterprise ready environment.

## Meeting long-term requirements while refactoring

The section of the Ready methodology on expanding your landing zone will aid in moving towards the longer term requirements. As the cloud adoption team progresses with their adoption plan, review [Expand your landing zone](#)) for guidance to help make decisions and refactor to meet the evolving requirements of various teams.

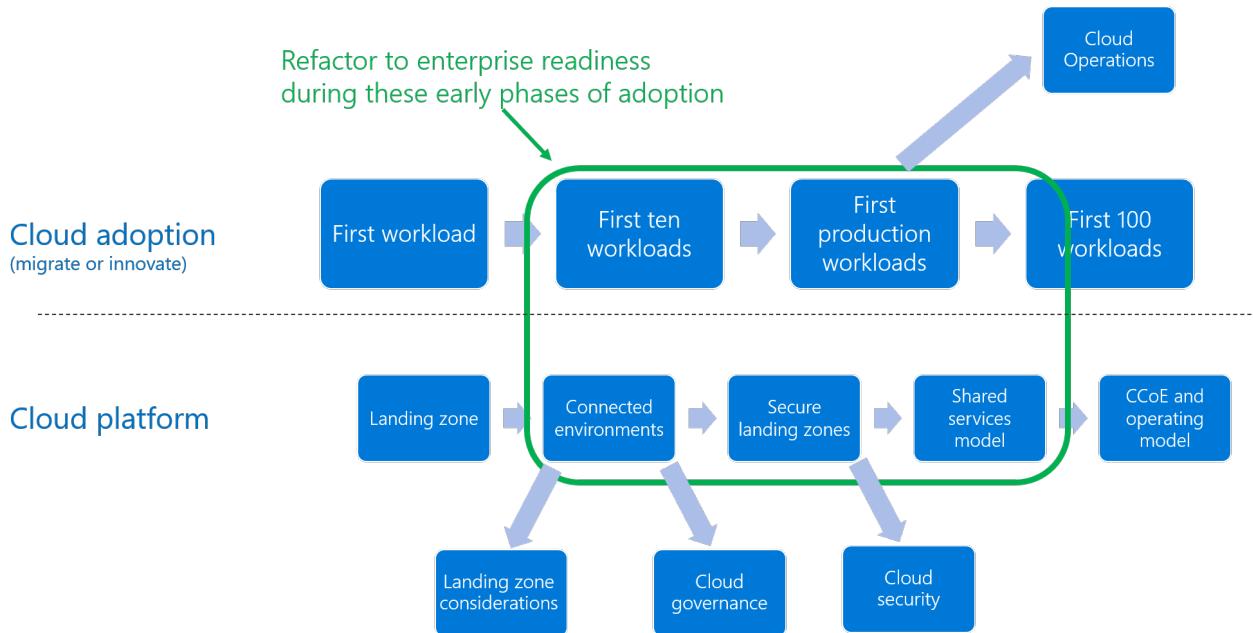


Figure 5: Deeper methodologies assisting a parallel landing zone iteration.

Each subsection of [Expand your landing zone](#) maps to one of the additions outlined in the image above. Beyond those basic expansions, the deeper methodologies (such as govern or manage) of this framework will aid in going beyond basic landing zone modifications to implement long-term disciplines.

## Next steps

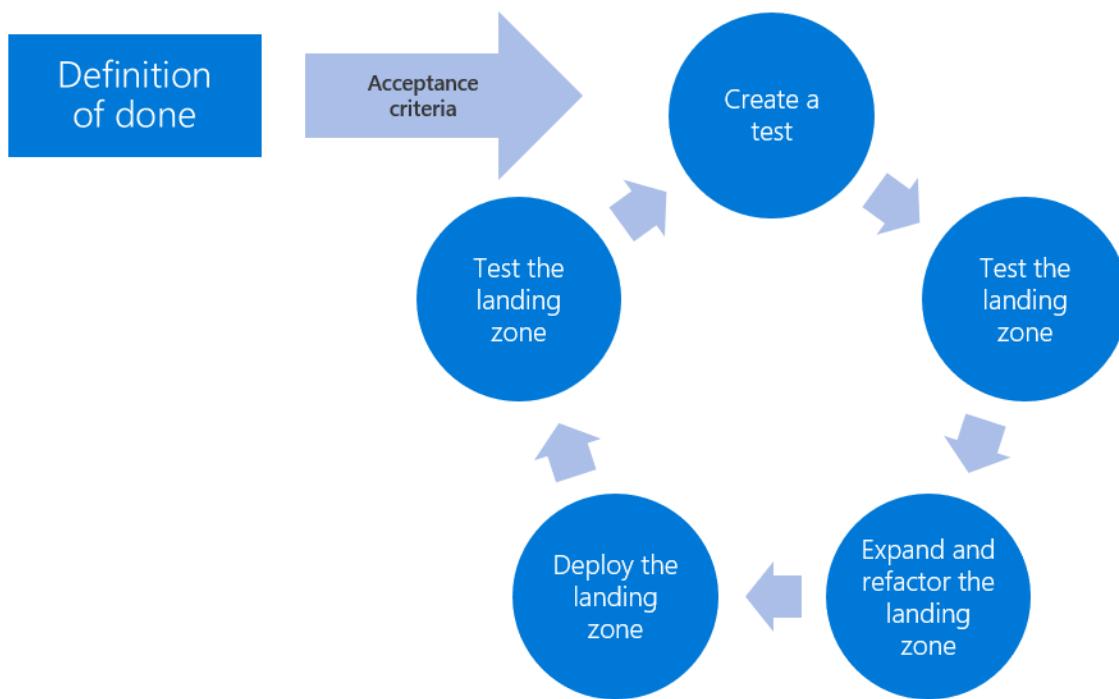
To get started on a refactoring process, get started using [Azure landing zones](#).

[Azure landing zones](#)

# Test-driven development (TDD) for landing zones

11/9/2020 • 5 minutes to read • [Edit Online](#)

Test-driven development is a common software development and DevOps process that improves the quality of new features and improvements in any code-based solution. Cloud-based infrastructure, and the underlying source code can use this process to ensure landing zones meet core requirements and are of high quality. This process is especially useful when landing zones are being developed and refactored in a parallel development effort.



In the cloud, infrastructure is the output of code execution. Well-structured, tested, and verified code produces a viable landing zone. A [landing zone](#) is an environment for hosting your workloads, preprovisioned through code. It includes foundational capabilities using a defined set of cloud services and best practices that set you up for success. This guidance describes an approach that uses test-driven development to fulfill the last part of that definition, while meeting quality, security, operations, and governance requirements.

This approach can be used to meet simple feature requests during early development. Later in the cloud adoption lifecycle, this process can be used to meet security, operations, governance, or compliance requirements.

## Definition of done

"Set up for success" is a subjective statement. This statement provides the cloud platform team with little actionable information during landing zone development or refactoring efforts. This lack of clarity can lead to missed expectations and vulnerabilities in a cloud environment. Before refactoring or expanding any landing zone, the cloud platform team should seek clarity regarding the "definition of done" for each landing zone.

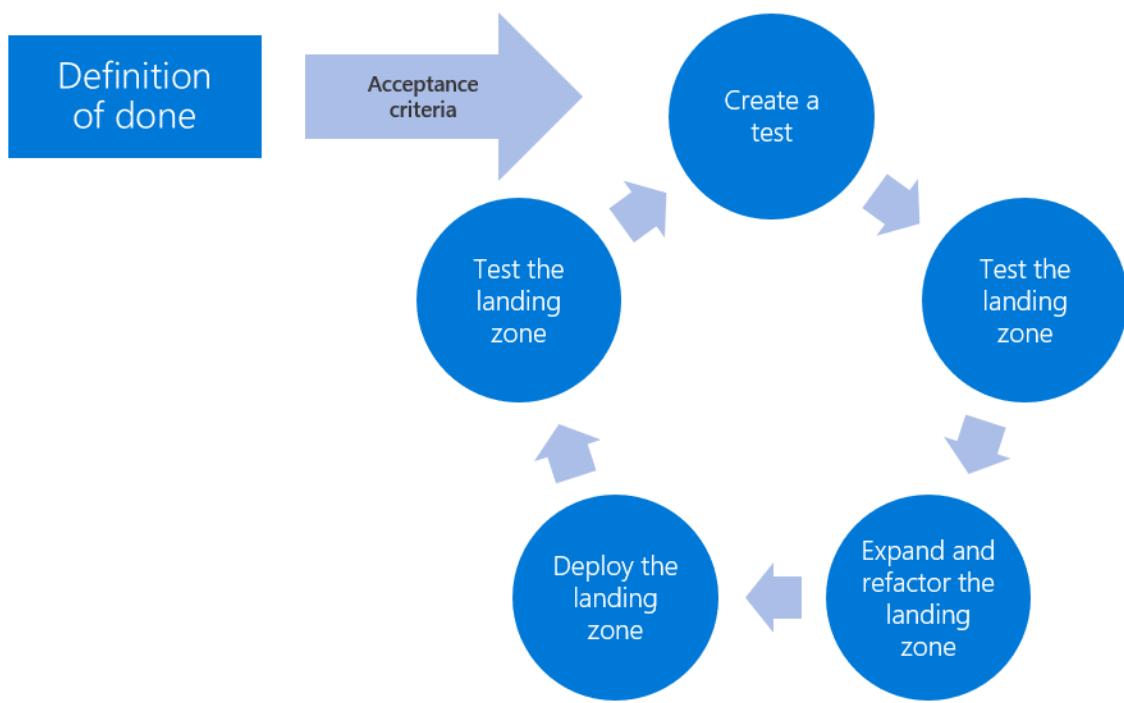
Definition of done is a simple agreement between the cloud platform team and other affected teams. This agreement outlines the expected value added features, which should be included in any landing zone development effort. The definition of done is often a checklist that's aligned with the short-term cloud adoption plan. In mature processes, those expected features in the checklist will each have their own acceptance criteria to

create even more clarity. When the value-added features each meet the acceptance criteria, the landing zone is sufficiently configured to enable the success of the current wave or release of adoption effort.

As teams adopt additional workloads and cloud features, the definition of done and acceptance criteria will become increasingly more complex.

## Test-driven development cycle

The cycle that makes test-driven development effective is often referred to as a red/green test. In this approach, the cloud platform team starts with a failed test (red test) based on the definition of done and defined acceptance criteria. For each feature or acceptance criteria, the cloud platform team would complete development tasks until the test passes (green test). A test-driven development cycle (or red/green test) would repeat the basic steps in the following image and list below until the full definition of done can be met.



- **Create a test:** Define a test to validate that acceptance criteria for a specific value-add feature has been met. Automate the test whenever possible.
- **Test the landing zone:** Run the new test and any existing tests. If the required feature hasn't already been met by prior development efforts and isn't inclusive to the cloud provider's offering, the test should fail. Running existing tests will help validate that your new test doesn't reduce reliability of landing zone features delivered by existing code.
- **Expand and refactor the landing zone:** Add or modify the source code to fulfill the requested value-add feature and improve the general quality of the code base. To meet the fullest spirit of test-driven development, the cloud platform team would only add code to meet the requested feature and nothing more. At the same time, code quality and maintenance is a shared effort. When fulfilling new feature requests, the cloud platform team should seek to improve the code by removing duplication and clarifying the code. Running tests between new code creation and refactoring of source code is highly suggested.
- **Deploy the landing zone:** Once the source code is capable of fulfilling the feature request, deploy the modified landing zone to the cloud provider in a controlled testing or sandbox environment.
- **Test the landing zone:** Retesting the landing zone should validate that the new code meets the acceptance criteria for the requested feature. Once all tests pass, the feature is considered complete and the acceptance criteria are considered to be met.

When all value-added features and acceptance criteria pass their associated tests, the landing zone is ready to support the next wave of the cloud adoption plan.

## Simple example of a definition of done

For an initial migration effort, definition of done may be overly simple. The following is an example of one of these overly simple examples.

- The initial landing zone will be used to host 10 workloads for initial learning purposes. These workloads are not critical to the business and have no access to sensitive data. In the future, it's likely these workloads will be released to production but criticality and sensitive is not expected to change. To support these workloads, the cloud adoption team will need the following criteria met:
  - Network segmentation to align with proposed network design.
  - Access to compute, storage, and networking resources to host the workloads aligned to the digital estate discovery.
  - Naming and tagging schema for ease of use.
  - This environment should be treated as a perimeter network with access to the public internet.
  - During adoption efforts, the cloud adoption team would like temporary access to the environment to change service configurations.
  - For awareness only: prior to production release, these workloads will require integration with the corporate identity provider to govern ongoing identity and access for operations management purposes. At which time the cloud adoption team's access should be revoked.

The last point above is not a feature or acceptance criteria. But it is an indicator that additional expansions will be required and should be explored with other teams early.

## Additional examples of a definition of done

The Govern methodology within the Cloud Adoption Framework provides a narrative journey through the natural maturity of a governance team. Embedded in that journey are several examples of "definition of done" and "acceptance criteria", in the form of policy statements.

- **Initial policy statements:** Example of corporate policies governing and initial definition of done based on early stage adoption requirements.
- **Identity expansion:** Example of corporate policies governing ("definition of done") to meet requirements to expand identity management for a landing zone.
- **Security expansion:** Example of corporate policies governing ("definition of done") to meet security requirements aligned to the reference cloud adoption plan.
- **Operations expansion:** Example of corporate policies governing ("definition of done") to meet basic operations management requirements.
- **Cost expansion:** Example of corporate policies governing ("definition of done") to meet cost management requirements.

The above examples are basic samples to help develop a "definition of done" for your landing zones. Additional sample policies are available for each of the [Five Disciplines of Cloud Governance](#).

## Next steps

To accelerate test-driven development in Azure, review [test-driven development features of Azure](#).

[Test-driven development in Azure](#)



# Test-driven development for landing zones in Azure

11/9/2020 • 3 minutes to read • [Edit Online](#)

As outlined in the previous article on [test-driven development \(TDD\) for landing zones](#), TDD cycles begin with a test that validates the acceptance criteria of a specific feature required to deliver the cloud adoption plan. Expanding or refactoring the landing zone can then be tested to validate that the acceptance criteria have been met. This article outlines a cloud-native toolchain in Azure to automate test-driven development cycles.

## Azure tools to support landing zone TDD cycles

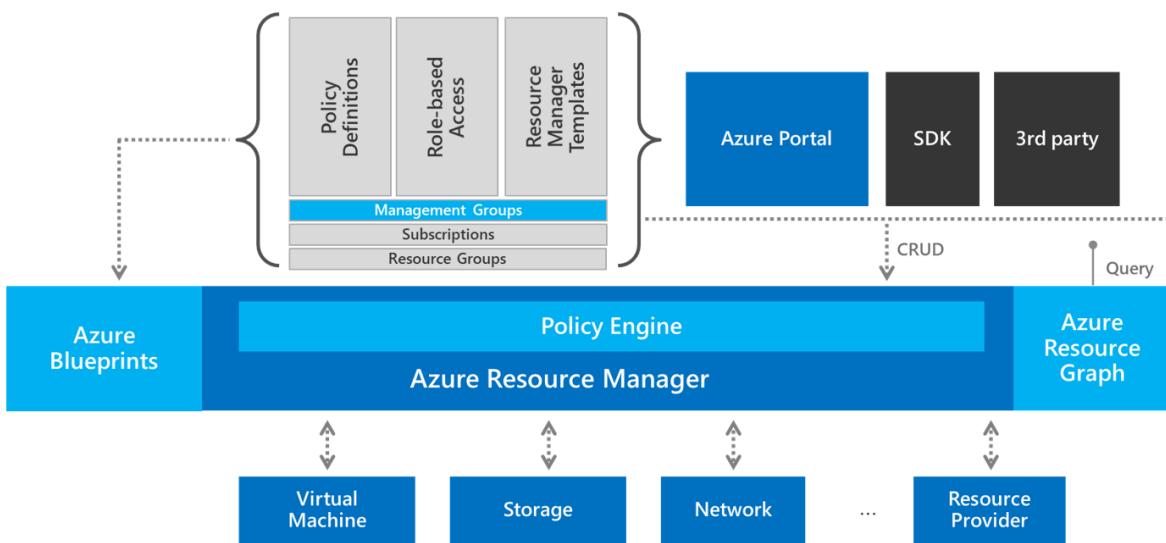


Figure 1: Test-driven development tools in Azure.

The toolchain of Azure-native governance products and services can be easily integrated into test-driven development for the creation of landing zones. Each of these tools serves a specific purpose, making it easier to develop, test, and deploy your landing zone in alignment with TDD cycles.

## Microsoft-provided test and deployment templates to accelerate TDD

The following examples are provided by Microsoft for governance purposes. Each can be used as a test or series of tests in a test-driven development cycle for landing zones. The following sections provide more information on each tool:

- Azure Blueprints provides various [blueprint samples](#), including policies for testing and templates for deployment. These blueprint samples can accelerate development, deployment, and testing efforts in TDD cycles.
- Azure Policy also includes [built-in policy initiatives](#), which could be used to test and enforce the full definition of done for a landing zone. Azure Policy includes [built-in policy definitions](#) that can meet individual acceptance criteria within the definition of done.
- Azure Graph includes advanced [query samples](#), which can be used to understand how the workloads are deployed within a landing zone for advanced testing scenarios.
- [Azure quickstart templates](#) provides source code templates to aid in accelerating landing zone and workload deployment.

The examples listed above can be used as tools for accelerating TDD cycles. They run on the governance tools in

the following sections and allow cloud platform teams to create their own source code and tests.

## Azure governance tools that can accelerate TDD cycles

**Azure Policy:** When deployments or attempted deployments deviate from governance policies, Azure Policy can provide automated detection, protection, and resolution. But Azure Policy also provides the primary mechanism for testing acceptance criteria in your definition of done. In a TDD cycle, a policy definition can be created to test a single acceptance criteria. Likewise, all acceptance criteria can be added to a policy initiative assigned to the entire subscription. This approach provides a mechanism for red tests before modifying the landing zone. Once the landing zone meets the definition of done, it can be used to enforce the test criteria to avoid code changes that would cause the test to fail in future releases.

**Azure Blueprints:** Azure blueprint groups policies and other deployment tools into a repeatable package that can be assigned to multiple landing zones. Blueprints prove useful when multiple adoption efforts share common definitions of done, which you may want to update over time. It can also help with deployment during subsequent efforts to expand and refactor landing zones.

**Azure Resource Graph:** Resource Graph provides a query language for creating data-driven tests based on information about the assets deployed within a landing zone. Later in the adoption plan, this tool can also define complex tests based on the interactions between workload assets and the underlying cloud environment.

**Azure Resource Manager templates:** These templates provide the primary source code for any environment deployed in Azure. Some third-party tools like Terraform generate their own ARM templates, which are then submitted to Azure Resource Manager.

**Azure Resource Manager:** Resource Manager provides a consistent platform for build and deploy functions. This platform can deploy landing zones based on source code definitions.

## Next steps

To begin refactoring your first landing zone, evaluate [basic landing zone considerations](#).

[Basic landing zone considerations](#)

# Best practices for Azure readiness

11/9/2020 • 3 minutes to read • [Edit Online](#)

Cloud readiness requires equipping staff with the technical skills needed to start a cloud adoption effort and prepare your migration target environment for the assets and workloads you'll move to the cloud. Read these best practices and additional guidance to help your team prepare your Azure environment.

## Azure fundamentals

Organize and deploy your assets in the Azure environment.

- [Azure fundamental concepts](#). Learn key Azure concepts and terms, and how these concepts relate to one another.
- [Create your initial subscriptions](#). Establish an initial set of Azure subscriptions to begin your cloud adoption.
- [Scale your Azure environment using multiple subscriptions](#). Understand reasons and strategies for creating additional subscriptions to scale your Azure environment.
- [Organize your resources with Azure management groups](#). Learn how Azure management groups can manage resources, roles, policies, and deployment across multiple subscriptions.
- [Follow recommended naming and tagging conventions](#). Review detailed recommendations for naming and tagging your resources. These recommendations support enterprise cloud adoption efforts.
- [Create hybrid cloud consistency](#). Create hybrid cloud solutions that provide the benefits of cloud innovation while maintaining many of the conveniences of on-premises management.

## Networking

Prepare your cloud networking infrastructure to support your workloads.

- [Networking decisions](#). Choose the networking services, tools, and architectures that will support your organization's workload, governance, and connectivity requirements.
- [Virtual network planning](#). Plan virtual networks based on your isolation, connectivity, and location requirements.
- [Best practices for network security](#). Learn best practices for addressing common network security issues using built-in Azure capabilities.
- [Perimeter networks](#). Enable secure connectivity between your cloud networks and your on-premises or physical datacenter networks, along with any connectivity to and from the internet.
- [Hub and spoke network topology](#). Efficiently manage common communication or security requirements for complicated workloads and address potential Azure subscription limitations.

## Identity and access control

Design your identity and access control infrastructure to improve the security and management efficiency of your workloads.

- [Azure identity management and access control security best practices](#). Learn best practices for identity management and access control using built-in Azure capabilities.
- [Best practices for role-based access control](#). Enable fine-grained and group-based access management for resources organized around user roles.
- [Securing privileged access for hybrid and cloud deployments in Azure Active Directory](#). Ensure that your organization's administrative access and privileged accounts are secure across your cloud and on-premises

environment.

## Storage

- [Azure Storage guidance](#). Select the right Azure Storage solution to support your usage scenarios.
- [Azure Storage security guide](#). Learn about security features in Azure Storage.

## Databases

- [Choose the correct SQL Server option in Azure](#). Choose the PaaS or IaaS solution that best supports your SQL Server workloads.
- [Database security best practices](#). Learn best practices for database security on the Azure platform.
- [Choose the right data store](#). Select the right data store to meet your requirements. Hundreds of implementation choices are available among SQL and NoSQL databases. Data stores are often categorized by how they structure data and the types of operations they support. This article describes several common storage models.

## Cost management

- [Tracking costs across business units, environments, and projects](#). Learn best practices for creating proper cost-tracking mechanisms.
- [How to optimize your cloud investment with Azure Cost Management and Billing](#). Implement a strategy for cost management and learn about the tools available for addressing cost challenges.
- [Create and manage budgets](#). Learn to create and manage budgets using Azure Cost Management and Billing.
- [Export cost data](#). Learn to export cost data using Azure Cost Management and Billing.
- [Optimize costs based on recommendations](#). Learn to identify underutilized resources and reduce costs by using Azure Cost Management and Billing and Azure Advisor.
- [Use cost alerts to monitor usage and spending](#). Learn to use Azure Cost Management and Billing alerts to monitor your Azure usage and spending.

# Create your initial Azure subscriptions

11/9/2020 • 2 minutes to read • [Edit Online](#)

Start your Azure adoption by creating an initial set of subscriptions. Learn what subscriptions you should begin with based on your initial requirements.

## Your first two subscriptions

Start by creating two subscriptions:

- Create one Azure subscription to contain your production workloads.
- Create a second subscription to serve as your nonproduction environment, using an [Azure Dev/Test offer](#) for lower pricing.



*Figure 1: An initial subscription model with keys next to boxes labeled "production" and "nonproduction".*

This approach has many benefits:

- Using separate subscriptions for your production and nonproduction environments creates a boundary that makes management of your resources simpler and safer.
- Azure Dev/Test subscription offerings are available for nonproduction workloads. These offerings provide discounted rates on Azure services and software licensing.
- Your production and nonproduction environments will likely have different sets of Azure policies. Using separate subscriptions makes it simple to apply each distinct policy at the subscription level.
- You can allow certain types of Azure resources in your nonproduction subscription for testing purposes. You can enable those resource providers in your nonproduction subscription without making them available in your production environment.
- You can use dev/test subscriptions as isolated sandbox environments. These sandboxes allow administrators and developers to rapidly build up and tear down entire sets of Azure resources. This isolation can also help with data protection and security concerns.
- The acceptable cost thresholds that you define will likely vary between production and dev/test subscriptions.

## Sandbox subscriptions

If innovation goals are part of your cloud adoption strategy, consider creating one or more sandbox subscriptions. You can apply security policies to keep these test subscriptions isolated from your production and nonproduction environments. Users can easily experiment with Azure capabilities in these isolated environments. Use an Azure Dev/Test offer to create these subscriptions.



Figure 2: A

*subscription model with sandbox subscriptions.*

## Shared services subscription

If you're planning to host more than 1,000 VMs or compute instances in the cloud within 24 months, create another Azure subscription to host shared services. This will prepare you to support your end-state enterprise architecture.

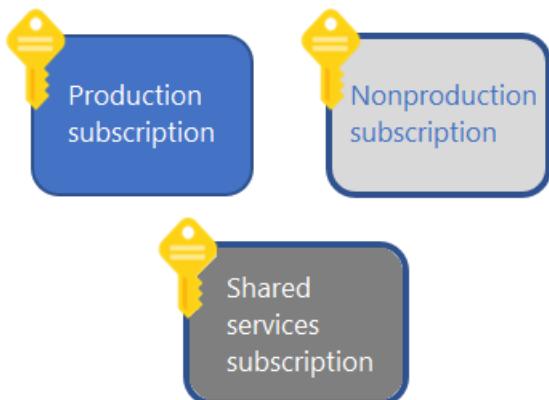


Figure 3: A subscription model with shared services.

## Next steps

Review the reasons why you might want to [create additional Azure subscriptions](#) to meet your requirements.

[Create additional subscriptions to scale your Azure environment](#)

# Create additional subscriptions to scale your Azure environment

11/9/2020 • 2 minutes to read • [Edit Online](#)

Organizations often use multiple Azure subscriptions to avoid per-subscription resource limits and to better manage and govern their Azure resources. It's important to define a strategy for scaling your subscriptions.

## Review fundamental concepts

As you expand your Azure environment beyond your [initial subscriptions](#), it's important to understand Azure concepts such as accounts, tenants, directories, and subscriptions. For more information, see [Azure fundamental concepts](#).

Other considerations might necessitate additional subscriptions. Keep the following in mind as you expand your cloud estate.

## Technical considerations

**Subscription limits:** Subscriptions have defined limits for some resource types. For example, the number of virtual networks in a subscription is limited. When a subscription approaches these limits, you'll need to create another subscription and put additional resources there. For more information, see [Azure subscription and service limits](#).

**Classic model resources:** If you've been using Azure for a long time, you may have resources that were created using the classic deployment model. Azure policies, role-based access control, resource grouping, and tags cannot be applied to classic model resources. You should move these resources into subscriptions that contain only classic model resources.

**Costs:** There might be some additional costs for data ingress and egress between subscriptions.

## Business priorities

Your business priorities might lead you to create additional subscriptions. These priorities include:

- Innovation
- Migration
- Cost
- Operations
- Security
- Governance

For other considerations about scaling your subscriptions, review the [subscription decision guide](#) in the Cloud Adoption Framework.

## Moving resources between subscriptions

As your subscription model grows, you might decide that some resources belong in other subscriptions. Many types of resources can be moved between subscriptions. You can also use automated deployments to re-create resources in another subscription. For more information, see [Move Azure resources to another resource group or subscription](#).

## Tips for creating new subscriptions

- Identify who is responsible for creating new subscriptions.
- Decide which resource types are available in a subscription by default.
- Decide what all standard subscriptions should look like. Considerations include RBAC access, policies, tags, and infrastructure resources.
- If possible, [programmatically create new subscriptions](#) via a service principal. You must [grant permission to the service principal](#) to create subscriptions. Define a security group that can request new subscriptions via an automated workflow.
- If you're an Enterprise Agreement (EA) customer, ask Azure support to block creation of non-EA subscriptions for your organization.

## Next steps

Create a management group hierarchy to help [organize and manage your subscriptions and resources](#).

[Organize and manage your subscriptions and resources](#)

# Organize and manage multiple Azure subscriptions

11/9/2020 • 2 minutes to read • [Edit Online](#)

If you have only a few subscriptions, then managing them independently is relatively simple. However, if you have many subscriptions, create a management group hierarchy to help manage your subscriptions and resources.

## Azure management groups

Azure management groups help you efficiently manage access, policies, and compliance for your subscriptions. Each management group is a container for one or more subscriptions.

Management groups are arranged in a single hierarchy. You define this hierarchy in your Azure Active Directory (Azure AD) tenant to align with your organization's structure and needs. The top level is called the *root management group*. You can define up to six levels of management groups in your hierarchy. Each subscription is contained by only one management group.

Azure provides four levels of management scope:

- Management groups
- Subscriptions
- Resource groups
- Resources

Any access or policy applied at one level in the hierarchy is inherited by the levels below it. A resource owner or subscription owner can't alter an inherited policy. This limitation helps improve governance.

### NOTE

Tag inheritance is not yet supported but will be available soon.

This inheritance model lets you arrange the subscriptions in your hierarchy so that each subscription follows appropriate policies and security controls.

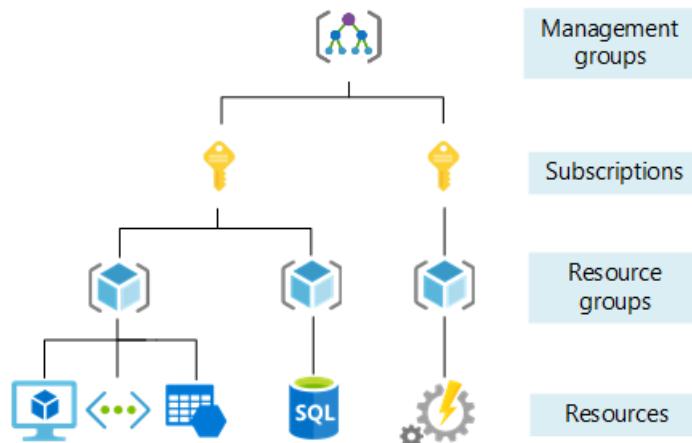


Figure 1: The four scope levels for organizing

your Azure resources.

Any access or policy assignment on the root management group applies to all resources in the directory. Carefully consider which items you define at this scope. Include only the assignments you must have.

# Create your management group hierarchy

When you define your management group hierarchy, first create the root management group. Then move all existing subscriptions in the directory into the root management group. New subscriptions are always created in the root management group. Later, you can move them to another management group.

When you move a subscription to an existing management group, it inherits the policies and role assignments from the management group hierarchy above it. Once you have established multiple subscriptions for your Azure workloads, you can create additional subscriptions to contain Azure services that other subscriptions share.

If you expect your Azure environment to grow, you should create management groups for production and nonproduction now, and apply appropriate policies and access controls at the management group level. New subscriptions will inherit the appropriate controls as they're added to each management group.

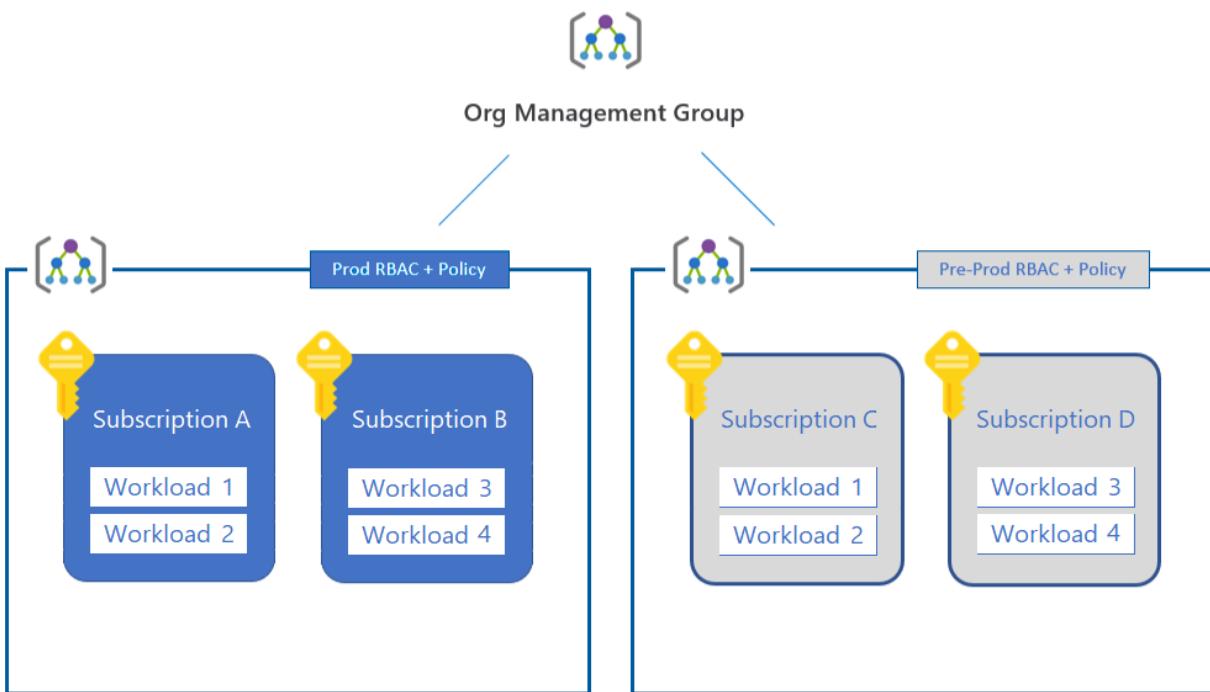


Figure 2: An example of a management group hierarchy.

## Example use cases

Some basic examples of using management groups to separate different workloads include:

**Production versus nonproduction workloads:** Use management groups to more easily manage different roles and policies between production and nonproduction subscriptions. For example, developers might have contributor access in production subscriptions but only reader access in nonproduction subscriptions.

**Internal services versus external services:** Enterprises often have different requirements, policies, and roles for internal services versus external customer-facing services.

## Related resources

Review the following resources to learn more about organizing and managing your Azure resources.

- [Organize your resources with Azure management groups](#)
- [Elevate access to manage all Azure subscriptions and management groups](#)
- [Move Azure resources to another resource group or subscription](#)

## Next steps

Review [recommended naming and tagging conventions](#) to follow when deploying your Azure resources.

[Recommended naming and tagging conventions](#)

# Recommended naming and tagging conventions

11/9/2020 • 11 minutes to read • [Edit Online](#)

Organize your cloud assets to support operational management and accounting requirements. Well-defined naming and metadata tagging conventions help to quickly locate and manage resources. These conventions also help associate cloud usage costs with business teams via chargeback and showback accounting mechanisms.

Accurate representation and naming of resources are critical for security purposes. In the event of a security incident, quickly identifying affected systems, their potential business impact, and what they are being used for is critical to making good risk decisions. Security services such as [Azure Security Center](#) and [Azure Sentinel](#) reference resources and their associated logging/alert information by resource name.

Azure defines [naming rules and restrictions for Azure resources](#). This guidance provides detailed recommendations to support enterprise cloud adoption efforts.

Changing resource names can be difficult. Establish a comprehensive naming convention before you begin any large cloud deployment.

## NOTE

Every business has different organizational and management requirements. These recommendations provide a starting point for discussions within your cloud adoption teams.

As these discussions proceed, use the following template to capture the naming and tagging decisions you make when you align these recommendations to your specific business needs.

Download the [naming and tagging conventions tracking template](#).

## Naming and tagging resources

A naming and tagging strategy includes business and operational details as components of resource names and metadata tags:

The business side of this strategy ensures that resource names and tags include the organizational information needed to identify the teams. Use a resource along with the business owners who are responsible for resource costs.

The operational side ensures that names and tags include information that IT teams use to identify the workload, application, environment, criticality, and other information useful for managing resources.

## Resource naming

An effective naming convention assembles resource names by using important resource information as parts of a resource's name. For example, using these [recommended naming conventions](#), a public IP resource for a production SharePoint workload is named like this: `pip-sharepoint-prod-westus-001`.

From the name, you can quickly identify the resource's type, its associated workload, its deployment environment, and the Azure region hosting it.

### Naming scope

All Azure resource types have a scope that defines the level that resource names must be unique. A resource must have a unique name within its scope.

For example, a virtual network has a resource group scope, which means that there can be only one network named `vnet-prod-westus-001` in a given resource group. Other resource groups could have their own virtual network named `vnet-prod-westus-001`. Subnets are scoped to virtual networks, so each subnet within a virtual network must be uniquely named.

Some resource names, such as PaaS services with public endpoints or virtual machine DNS labels, have global scopes, which means that they must be unique across the entire Azure platform.

Resource names have length limits. Balancing the context embedded in a name with its scope and length is important when you develop your naming conventions. For more information, see [naming rules and restrictions for Azure resources](#).

### Recommended naming components

When you construct your naming convention, identify the key pieces of information that you want to reflect in a resource name. Different information is relevant for different resource types. The following list provides examples of information that are useful when you construct resource names.

Keep the length of naming components short to prevent exceeding resource name length limits.

NAMING COMPONENT	DESCRIPTION	EXAMPLES
Business unit	Top-level division of your company that owns the subscription or workload the resource belongs to. In smaller organizations, this component might represent a single corporate top-level organizational element.	<code>fin</code> , <code>mktg</code> , <code>product</code> , <code>it</code> , <code>corp</code>
Subscription type	Summary description of the purpose of the subscription that contains the resource. Often broken down by deployment environment type or specific workloads.	<code>prod</code> , <code>shared</code> , <code>client</code>
Application or service name	Name of the application, workload, or service that the resource is a part of.	<code>navigator</code> , <code>emissions</code> , <code>sharepoint</code> , <code>hadoop</code>
Deployment environment	The stage of the development lifecycle for the workload that the resource supports.	<code>prod</code> , <code>dev</code> , <code>qa</code> , <code>stage</code> , <code>test</code>
Region	The Azure region where the resource is deployed.	<code>westus</code> , <code>eastus2</code> , <code>westeurope</code> , <code>usgovia</code>

### Recommended resource-type prefixes

Each workload can consist of many individual resources and services. Incorporating resource type prefixes into your resource names makes it easier to visually identify application or service components.

This list recommends Azure resource type prefixes to use when you define your naming conventions.

#### General

ASSET TYPE	NAME PREFIX
Management group	mg-

ASSET TYPE	NAME PREFIX
Resource group	rg-
Policy definition	policy-
API management service instance	apim-
Managed Identity	id-

## Networking

ASSET TYPE	NAME PREFIX
Virtual network	vnet-
Subnet	snet-
Virtual network peering	peer-
Network interface (NIC)	nic-
Public IP address	pip-
Load balancer (internal)	lbi-
Load balancer (external)	lbe-
Network security group (NSG)	nsg-
Application security group (ASG)	asg-
Local network gateway	lgw-
Virtual network gateway	vgw-
VPN connection	cn-
ExpressRoute circuit	erc-
Application gateway	agw-
Route table	route-
User defined route (UDR)	udr-
Traffic Manager profile	traf-
Front door	fd-
CDN profile	cdnp-

ASSET TYPE	NAME PREFIX
CDN endpoint	cdne-
Web Application Firewall (WAF) policy	waf

## Compute and Web

ASSET TYPE	NAME PREFIX
Virtual machine	vm
Virtual machine scale set	vmss-
Availability set	avail-
Managed disk (OS)	osdisk
Managed disk (data)	disk
VM storage account	stvm
Azure Arc enabled server	arcs-
Azure Arc enabled Kubernetes cluster	arck
Container registry	cr
Container instance	ci-
AKS cluster	aks-
Service Fabric cluster	sf-
App Service environment	ase-
App Service plan	plan-
Web app	app-
Function app	func-
Cloud service	cld-
Notification Hubs	ntf-
Notification Hubs namespace	ntfns-

## Databases

ASSET TYPE	NAME PREFIX
Azure SQL Database server	sql-

ASSET TYPE	NAME PREFIX
Azure SQL database	sqldb-
Azure Cosmos DB database	cosmos-
Azure Cache for Redis instance	redis-
MySQL database	mysql-
PostgreSQL database	psql-
Azure SQL Data Warehouse	sqldw-
Azure Synapse Analytics	syn-
SQL Server Stretch Database	sqlstrdb-
SQL Managed Instance	sqlmi-

## Storage

ASSET TYPE	NAME PREFIX
Storage account	st
Azure StorSimple	ssimp
Azure Container Registry	acr

## AI and Machine Learning

ASSET TYPE	NAME PREFIX
Azure Cognitive Search	srch-
Azure Cognitive Services	cog-
Azure Machine Learning workspace	mlw-

## Analytics and IoT

ASSET TYPE	NAME PREFIX
Azure Analysis Services server	as
Azure Databricks workspace	dbw-
Azure Stream Analytics	asa-
Azure Data Explorer cluster	dec
Azure Data Factory	adf-

ASSET TYPE	NAME PREFIX
Data Lake Store account	dls
Data Lake Analytics account	dla
Event hub	evh-
HDInsight - Hadoop cluster	hadoop-
HDInsight - HBase cluster	hbase-
HDInsight - Kafka cluster	kafka-
HDInsight - Spark cluster	spark-
HDInsight - Storm cluster	storm-
HDInsight - ML Services cluster	mls-
IoT hub	iot-
Power BI Embedded	pbi-
Time Series Insights environment	tsi-

## Developer tools

ASSET TYPE	NAME PREFIX
App Configuration store	appcs-

## Integration

ASSET TYPE	NAME PREFIX
Integration account	ia-
Logic apps	logic-
Service Bus	sb-
Service Bus queue	sbq-
Service Bus topic	sbt-

## Management and governance

ASSET TYPE	NAME PREFIX
Automation account	aa-
Azure Monitor action group	ag-

ASSET TYPE	NAME PREFIX
Blueprint	bp-
Blueprint assignment	bpa-
Key vault	kv-
Log Analytics workspace	log-
Application Insights	appi-
Recovery Services vault	rsv-

## Migration

ASSET TYPE	NAME PREFIX
Azure Migrate project	migr-
Database Migration Service instance	dms-
Recovery Services vault	rsv-

## Metadata tags

When you apply metadata tags to your cloud resources, you can include information about those assets that couldn't be included in the resource name. You can use that information to perform more sophisticated filtering and reporting on resources. You want these tags to include context about the resource's associated workload or application, operational requirements, and ownership information. This information can be used by IT or business teams to find resources or generate reports about resource usage and billing.

What tags you apply to resources and what tags are required or optional differs among organizations. The following list provides examples of common tags that capture important context and information about a resource. Use this list as a starting point to establish your own tagging conventions.

TAG NAME	DESCRIPTION	KEY	EXAMPLE VALUE
Application name	Name of the application, service, or workload the resource is associated with.	<i>ApplicationName</i>	{application name}
Approver name	Person responsible for approving costs related to this resource.	<i>Approver</i>	{email}
Budget required/approved	Money allocated for this application, service, or workload.	<i>BudgetAmount</i>	{\$}

Tag name	Description	Key	Example value
Business unit	Top-level division of your company that owns the subscription or workload the resource belongs to. In smaller organizations, this tag might represent a single corporate or shared top-level organizational element.	<i>BusinessUnit</i>	<i>FINANCE, MARKETING, {Product Name}, CORP, SHARED</i>
Cost center	Accounting cost center associated with this resource.	<i>CostCenter</i>	{number}
Disaster recovery	Business criticality of the application, workload, or service.	<i>DR</i>	<i>Mission-critical, Critical, Essential</i>
End date of the project	Date when the application, workload, or service is scheduled for retirement.	<i>EndDate</i>	{date}
Environment	Deployment environment of the application, workload, or service.	<i>Env</i>	<i>Prod, Dev, QA, Stage, Test</i>
Owner name	Owner of the application, workload, or service.	<i>Owner</i>	{email}
Requester name	User who requested the creation of this application.	<i>Requester</i>	{email}
Service class	Service level agreement level of the application, workload, or service.	<i>ServiceClass</i>	<i>Dev, Bronze, Silver, Gold</i>
Start date of the project	Date when the application, workload, or service was first deployed.	<i>StartDate</i>	{date}

## Example names

The following section provides some example names for common Azure resource types in an enterprise cloud deployment.

### Example names: General

Asset type	Scope	Format	Examples
Management group	Business unit and/or Environment type	mg-<Business Unit>[-<Environment type>]	<ul style="list-style-type: none"> <li>• mg-mktg</li> <li>• mg-hr</li> <li>• mg-corp-prod</li> <li>• mg-fin-client</li> </ul>

ASSET TYPE	SCOPE	FORMAT	EXAMPLES
Subscription	Account/ Enterprise Agreement	<Business Unit>- <Subscription type>- <###>	<ul style="list-style-type: none"> <li>• mktg-prod-001</li> <li>• corp-shared-001</li> <li>• fin-client-001</li> </ul>
Resource group	Subscription	rg-<App or service name>-<Subscription type>-<###>	<ul style="list-style-type: none"> <li>• rg-mktgsharepoint- prod-001</li> <li>• rg-acctlookupsvc-share- 001</li> <li>• rg-ad-dir-services- shared-001</li> </ul>
API management service instance	Global	apim-<App or service name>	apim-navigator-prod
Managed Identity	Resource group	id-<App or service name>	id-appcn-keda-prod-eus- 001

#### NOTE

The example names above and elsewhere in this document reference a three digit padding (<###>). I.E. mktg-prod-001

Padding aids in human readability and sorting of assets when those assets are managed in a configuration management database (CMDB), IT Asset Management tool, or traditional accounting tools. When the deployed asset is managed centrally as part of a larger inventory or portfolio of IT assets, the padding approach aligns with interfaces those systems use to manage inventory naming.

Unfortunately, the traditional asset padding approach can prove problematic in infrastructure-as-code approaches which may iterate through assets based on a non-padded number. This approach is common during deployment or automated configuration management tasks. Those scripts would have to routinely strip the padding and convert the padded number to a real number, which slows script development and run time.

Which approach you choose to implement is a personal decision. The padding in this article is meant to illustrate the importance of using a consistent approach to inventory numbering, not which approach is superior. Before deciding on a number schema (with or without padding) evaluate which will have a bigger impact on long term operations: CMDB/asset management solutions or code-based inventory management. Then consistently follow the padding option that best fits your operational needs.

#### Example names: Networking

ASSET TYPE	SCOPE	FORMAT	EXAMPLES
Virtual network	Resource group	vnet-<Subscription type>- <Region>-<###>	<ul style="list-style-type: none"> <li>• vnet-shared-eastus2-001</li> <li>• vnet-prod-westus-001</li> <li>• vnet-client-eastus2-001</li> </ul>
Subnet	Virtual network	snet-<subscription>- <subregion>-<###>	<ul style="list-style-type: none"> <li>• snet-shared-eastus2-001</li> <li>• snet-prod-westus-001</li> <li>• snet-client-eastus2-001</li> </ul>

ASSET TYPE	SCOPE	FORMAT	EXAMPLES
Network interface (NIC)	Resource group	nic-<##>-<vm name>-<subscription>-<###>	<ul style="list-style-type: none"> <li>• nic-01-dc1-shared-001</li> <li>• nic-02-vmhadoop1-prod-001</li> <li>• nic-02-vmtest1-client-001</li> </ul>
Public IP address	Resource group	pip-<vm name or app name>-<Environment>-<subregion>-<###>	<ul style="list-style-type: none"> <li>• pip-dc1-shared-eastus2-001</li> <li>• pip-hadoop-prod-westus-001</li> </ul>
Load balancer	Resource group	lb-<app name or role><Environment><###>	<ul style="list-style-type: none"> <li>• lb-navigator-prod-001</li> <li>• lb-sharepoint-dev-001</li> </ul>
Network security group (NSG)	Subnet or NIC	nsg-<policy name or app name>-<###>	<ul style="list-style-type: none"> <li>• nsg-weballow-001</li> <li>• nsg-rdpallow-001</li> <li>• nsg-sqlallow-001</li> <li>• nsg-dnsblocked-001</li> </ul>
Local network gateway	Virtual gateway	lgw-<Subscription type>-<Region>-<###>	<ul style="list-style-type: none"> <li>• lgw-shared-eastus2-001</li> <li>• lgw-prod-westus-001</li> <li>• lgw-client-eastus2-001</li> </ul>
Virtual network gateway	Virtual network	vgw-<Subscription type>-<Region>-<###>	<ul style="list-style-type: none"> <li>• vgw-shared-eastus2-001</li> <li>• vgw-prod-westus-001</li> <li>• vgw-client-eastus2-001</li> </ul>
Site-to-site connection	Resource group	cn-<local gateway name>-to-<virtual gateway name>	<ul style="list-style-type: none"> <li>• cn-lgw-shared-eastus2-001-to-vgw-shared-eastus2-001</li> <li>• cn-lgw-shared-eastus2-001-to-shared-westus-001</li> </ul>
VPN connection	Resource group	cn-<subscription1>-<region1>-to-<subscription2>-<region2>-	<ul style="list-style-type: none"> <li>• cn-shared-eastus2-to-shared-westus</li> <li>• cn-prod-eastus2-to-prod-westus</li> </ul>
Route table	Resource group	route-<route table name>	<ul style="list-style-type: none"> <li>• route-navigator</li> <li>• route-sharepoint</li> </ul>
DNS label	Global	<A record of vm>. <region>.cloudapp.azure.com	dc1.westus.cloudapp.azure.com web1.eastus2.cloudapp.azure.com

#### Example names: Compute and Web

ASSET TYPE	SCOPE	FORMAT	EXAMPLES
Virtual machine	Resource group	vm<policy name or app name><###>	<ul style="list-style-type: none"> <li>• vmnavigator001</li> <li>• vmsharepoint001</li> <li>• vmsqlnode001</li> <li>• vmhadoop001</li> </ul>

ASSET TYPE	SCOPE	FORMAT	EXAMPLES
VM storage account	Global	stvm<performance type>-<app name or prod name>-<region><###>	<ul style="list-style-type: none"> <li>stvmscoreeastus2001</li> <li>stvmpcoreeastus2001</li> <li>stvmstplmeastus2001</li> <li>stvmsdadoeastus2001</li> </ul>
Web app	Global	app-<App Name>-<Environment>-<###>. [{azurewebsites.net}]	<ul style="list-style-type: none"> <li>app-navigator-prod-001.azurewebsites.net</li> <li>app-accountlookup-dev-001.azurewebsites.net</li> </ul>
Function app	Global	func-<App Name>-<Environment>-<###>. [{azurewebsites.net}]	<ul style="list-style-type: none"> <li>func-navigator-prod-001.azurewebsites.net</li> <li>func-accountlookup-dev-001.azurewebsites.net</li> </ul>
Cloud service	Global	cld-<App Name>-<Environment>-<###>. [{cloudapp.net}]	<ul style="list-style-type: none"> <li>cld-navigator-prod-001.azurewebsites.net</li> <li>cld-accountlookup-dev-001.azurewebsites.net</li> </ul>
Notification hub	Resource group	ntf-<App Name>-<Environment>	<ul style="list-style-type: none"> <li>ntf-navigator-prod</li> <li>ntf-emissions-dev</li> </ul>
Notification Hubs namespace	Global	ntfns-<App Name>-<Environment>	<ul style="list-style-type: none"> <li>ntfns-navigator-prod</li> <li>ntfns-emissions-dev</li> </ul>

#### Example names: Databases

ASSET TYPE	SCOPE	FORMAT	EXAMPLES
Azure SQL Database server	Global	sql-<App Name>-<Environment>	<ul style="list-style-type: none"> <li>sql-navigator-prod</li> <li>sql-emissions-dev</li> </ul>
Azure SQL database	Azure SQL Database	sqldb-<Database Name>-<Environment>	<ul style="list-style-type: none"> <li>sqldb-users-prod</li> <li>sqldb-users-dev</li> </ul>
Azure Cosmos DB database	Global	cosmos-<App Name>-<Environment>	<ul style="list-style-type: none"> <li>cosmos-navigator-prod</li> <li>cosmos-emissions-dev</li> </ul>
Azure Cache for Redis instance	Global	redis-<App Name>-<Environment>	<ul style="list-style-type: none"> <li>redis-navigator-prod</li> <li>redis-emissions-dev</li> </ul>
MySQL database	Global	mysql-<App Name>-<Environment>	<ul style="list-style-type: none"> <li>mysql-navigator-prod</li> <li>mysql-emissions-dev</li> </ul>
PostgreSQL database	Global	psql-<App Name>-<Environment>	<ul style="list-style-type: none"> <li>psql-navigator-prod</li> <li>psql-emissions-dev</li> </ul>
Azure SQL Data Warehouse	Global	sqldw-<App Name>-<Environment>	<ul style="list-style-type: none"> <li>sqldw-navigator-prod</li> <li>sqldw-emissions-dev</li> </ul>
SQL Server Stretch Database	Azure SQL Database	sqlstrdb-<App Name>-<Environment>	<ul style="list-style-type: none"> <li>sqlstrdb-navigator-prod</li> <li>sqlstrdb-emissions-dev</li> </ul>

#### Example names: Storage

ASSET TYPE	SCOPE	FORMAT	EXAMPLES
Storage account (general use)	Global	st<storage name><###>	<ul style="list-style-type: none"> <li>• stnavigatordata001</li> <li>• stemissionsoutput001</li> </ul>
Storage account (diagnostic logs)	Global	stdiag<first 2 letters of subscription name and number><region><###>	<ul style="list-style-type: none"> <li>• stdiagh001eastus2001</li> <li>• stdiagh001westus001</li> </ul>
Azure StorSimple	Global	ssimp<App Name><Environment>	<ul style="list-style-type: none"> <li>• ssimpnavigatorprod</li> <li>• ssimpemissionsdev</li> </ul>
Azure Container Registry	Global	acr<App Name><Environment><###>	<ul style="list-style-type: none"> <li>• acrnavigatorprod001</li> </ul>

#### Example names: AI and machine learning

ASSET TYPE	SCOPE	FORMAT	EXAMPLES
Azure Cognitive Search	Global	srch-<App Name>-<Environment>	<ul style="list-style-type: none"> <li>• srch-navigator-prod</li> <li>• srch-emissions-dev</li> </ul>
Azure Cognitive Services	Resource group	cog-<App Name>-<Environment>	<ul style="list-style-type: none"> <li>• cog-navigator-prod</li> <li>• cog-emissions-dev</li> </ul>
Azure Machine Learning workspace	Resource group	mlw-<App Name>-<Environment>	<ul style="list-style-type: none"> <li>• mlw-navigator-prod</li> <li>• mlw-emissions-dev</li> </ul>

#### Example names: Analytics and IoT

ASSET TYPE	SCOPE	FORMAT	EXAMPLES
Azure Data Factory	Global	adf-<App Name>-<Environment>	<ul style="list-style-type: none"> <li>• adf-navigator-prod</li> <li>• adf-emissions-dev</li> </ul>
Azure Stream Analytics	Resource group	asa-<App Name>-<Environment>	<ul style="list-style-type: none"> <li>• asa-navigator-prod</li> <li>• asa-emissions-dev</li> </ul>
Data Lake Analytics account	Global	dla<App Name>-<Environment>	<ul style="list-style-type: none"> <li>• dlanavigatorprod</li> <li>• dlaemissionsdev</li> </ul>
Data Lake Storage account	Global	dls<App Name>-<Environment>	<ul style="list-style-type: none"> <li>• dlsnavigatorprod</li> <li>• dlsemissionsdev</li> </ul>
Event hub	Global	evh-<App Name>-<Environment>	<ul style="list-style-type: none"> <li>• evh-navigator-prod</li> <li>• evh-emissions-dev</li> </ul>
HDInsight - HBase cluster	Global	hbase-<App Name>-<Environment>	<ul style="list-style-type: none"> <li>• hbase-navigator-prod</li> <li>• hbase-emissions-dev</li> </ul>
HDInsight - Hadoop cluster	Global	hadoop-<App Name>-<Environment>	<ul style="list-style-type: none"> <li>• hadoop-navigator-prod</li> <li>• hadoop-emissions-dev</li> </ul>
HDInsight - Spark cluster	Global	spark-<App Name>-<Environment>	<ul style="list-style-type: none"> <li>• spark-navigator-prod</li> <li>• spark-emissions-dev</li> </ul>

ASSET TYPE	SCOPE	FORMAT	EXAMPLES
IoT hub	Global	iot-<App Name>-<Environment>	<ul style="list-style-type: none"> <li>• iot-navigator-prod</li> <li>• iot-emissions-dev</li> </ul>
Power BI Embedded	Global	pbi-<App Name>-<Environment>	<ul style="list-style-type: none"> <li>• pbi-navigator-prod</li> <li>• pbi-emissions-dev</li> </ul>

#### Example names: Integration

ASSET TYPE	SCOPE	FORMAT	EXAMPLES
Service Bus	Global	sb-<App Name>-<Environment>. [{servicebus.windows.net}]	<ul style="list-style-type: none"> <li>• sb-navigator-prod</li> <li>• sb-emissions-dev</li> </ul>
Service Bus queue	Service Bus	sbq-<query descriptor>	<ul style="list-style-type: none"> <li>• sbq-messagequery</li> </ul>
Service Bus topic	Service Bus	sbt-<query descriptor>	<ul style="list-style-type: none"> <li>• sbt-messagequery</li> </ul>

# The virtual datacenter: A network perspective

11/9/2020 • 43 minutes to read • [Edit Online](#)

Applications migrated from on-premises will benefit from Azure's secure cost-efficient infrastructure, even with minimal application changes. Even so, enterprises should adapt their architectures to improve agility and take advantage of Azure's capabilities.

Microsoft Azure delivers hyperscale services and infrastructure with enterprise-grade capabilities and reliability. These services and infrastructure offer many choices in hybrid connectivity, so customers can choose to access them over the internet or a private network connection. Microsoft partners can also provide enhanced capabilities by offering security services and virtual appliances that are optimized to run in Azure.

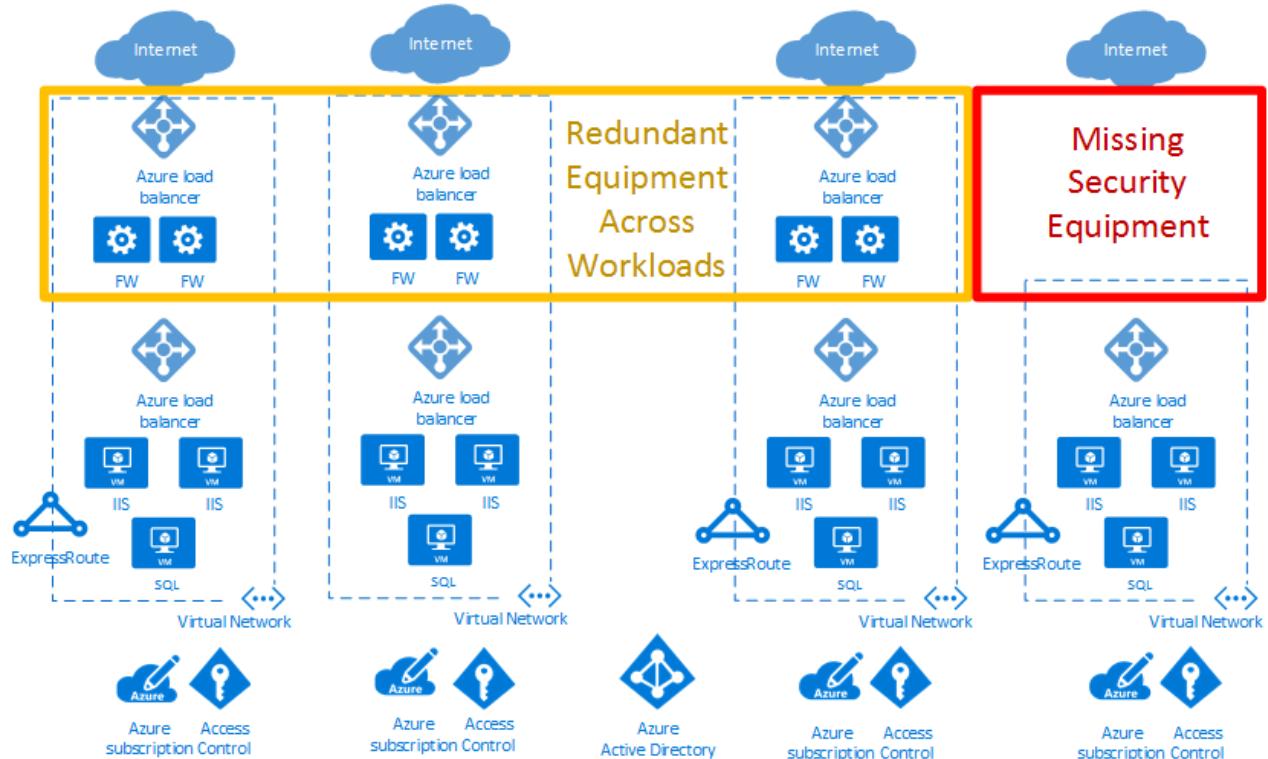
Customers can use Azure to seamlessly extend their infrastructure into the cloud and build multitier architectures.

## What is a virtual datacenter?

The cloud began as a platform for hosting public-facing applications. Enterprises recognized the value of the cloud and began migrating internal line-of-business applications. These applications brought additional security, reliability, performance, and cost considerations that required additional flexibility when delivering cloud services. New infrastructure and networking services were designed to provide this flexibility, and new features provided for elastic scale, disaster recovery, and other considerations.

Cloud solutions were initially designed to host single, relatively isolated applications in the public spectrum. This approach worked well for a few years. As the benefits of cloud solutions became clear, multiple large-scale workloads were hosted on the cloud. Addressing security, reliability, performance, and cost concerns of deployments in one or more regions became vital throughout the lifecycle of the cloud service.

In the example cloud deployment diagram below, the red box highlights a security gap. The yellow box shows an opportunity to optimize network virtual appliances across workloads.



Virtual datacenters help achieve the scale required for enterprise workloads. This scale must address the challenges introduced when running large-scale applications in the public cloud.

A virtual datacenter (VDC) implementation includes more than the application workloads in the cloud. It also provides the network, security, management, and other infrastructure such as DNS and Active Directory services. As enterprises migrate additional workloads to Azure, consider the infrastructure and objects that support these workloads. Carefully structuring your resources helps avoid proliferation of hundreds of separately managed "workload islands" with independent data flows, security models, and compliance challenges.

The virtual datacenter concept provides recommendations and high-level designs for implementing a collection of separate but related entities. These entities often have common supporting functions, features, and infrastructure. Viewing your workloads as a virtual datacenter helps realize reduced cost from economies of scale, optimized security via component and data flow centralization, and easier operations, management, and compliance audits.

#### **NOTE**

A virtual datacenter is **not** a specific Azure service. Rather, various Azure features and capabilities are combined to meet your requirements. A virtual datacenter is a way of thinking about your workloads and Azure usage to optimize your resources and capabilities in the cloud. It provides a modular approach to providing IT services in Azure while respecting the enterprise's organizational roles and responsibilities.

A virtual datacenter helps enterprises deploy workloads and applications in Azure for the following scenarios:

- Host multiple related workloads.
- Migrate workloads from an on-premises environment to Azure.
- Implement shared or centralized security and access requirements across workloads.
- Mix DevOps and centralized IT appropriately for a large enterprise.

## Who should implement a virtual datacenter?

Any customer that has decided to adopt Azure can benefit from the efficiency of configuring a set of resources for common use by all applications. Depending on the size, even single applications can benefit from using the patterns and components used to build a VDC implementation.

Some organizations have centralized teams or departments for IT, networking, security, or compliance. Implementing a VDC can help enforce policy points, separate responsibilities, and ensure the consistency of the underlying common components. Application teams can retain the freedom and control that is suitable for their requirements.

Organizations with a DevOps approach can also use VDC concepts to provide authorized pockets of Azure resources. This method can ensure the DevOps groups have total control within that grouping, at either the subscription level or within resource groups in a common subscription. At the same time, the network and security boundaries stay compliant as defined by a centralized policy in the hub network and centrally managed resource group.

## Considerations for implementing a virtual datacenter

When designing a virtual datacenter, consider these pivotal issues:

### **Identity and directory service**

Identity and directory services are key capabilities of both on-premises and cloud datacenters. Identity covers all aspects of access and authorization to services within a VDC implementation. To ensure that only authorized users and processes access your Azure resources, Azure uses several types of credentials for authentication, including account passwords, cryptographic keys, digital signatures, and certificates. [Azure Multi-Factor Authentication](#)

provides an additional layer of security for accessing Azure services using strong authentication with a range of easy verification options (phone call, text message, or mobile app notification) that allow customers to choose the method they prefer.

Any large enterprise needs to define an identity management process that describes the management of individual identities, their authentication, authorization, roles, and privileges within or across their VDC. The goals of this process should be to increase security and productivity while reducing cost, downtime, and repetitive manual tasks.

Enterprise organizations may require a demanding mix of services for different lines of business, and employees often have different roles when involved with different projects. The VDC requires good cooperation between different teams, each with specific role definitions, to get systems running with good governance. The matrix of responsibilities, access, and rights can be complex. Identity management in the VDC is implemented through [Azure Active Directory \(Azure AD\)](#) and role-based access control (RBAC).

A directory service is a shared information infrastructure that locates, manages, administers, and organizes everyday items and network resources. These resources can include volumes, folders, files, printers, users, groups, devices, and other objects. Each resource on the network is considered an object by the directory server. Information about a resource is stored as a collection of attributes associated with that resource or object.

All Microsoft online business services rely on Azure Active Directory (Azure AD) for sign-on and other identity needs. Azure Active Directory is a comprehensive, highly available identity and access management cloud solution that combines core directory services, advanced identity governance, and application access management. Azure AD can integrate with on-premises Active Directory to enable single sign-on for all cloud-based and locally hosted on-premises applications. The user attributes of on-premises Active Directory can be automatically synchronized to Azure AD.

A single global administrator isn't required to assign all permissions in a VDC implementation. Instead, each specific department, group of users, or services in the Directory Service can have the permissions required to manage their own resources within a VDC implementation. Structuring permissions requires balancing. Too many permissions can impede performance efficiency, and too few or loose permissions can increase security risks. Azure role-based access control (RBAC) helps to address this problem, by offering fine-grained access management for resources in a VDC implementation.

## Security infrastructure

Security infrastructure refers to the segregation of traffic in a VDC implementation's specific virtual network segment. This infrastructure specifies how ingress and egress are controlled in a VDC implementation. Azure is based on a multitenant architecture that prevents unauthorized and unintentional traffic between deployments by using virtual network isolation, access control lists, load balancers, IP filters, and traffic flow policies. Network address translation (NAT) separates internal network traffic from external traffic.

The Azure fabric allocates infrastructure resources to tenant workloads and manages communications to and from virtual machines (VMs). The Azure hypervisor enforces memory and process separation between VMs and securely routes network traffic to guest OS tenants.

## Connectivity to the cloud

A virtual datacenter requires connectivity to external networks to offer services to customers, partners, or internal users. This need for connectivity refers not only to the Internet, but also to on-premises networks and datacenters.

Customers control which services can access and be accessed from the public internet. This access is controlled by using [Azure Firewall](#) or other types of virtual network appliances (NVAs), custom routing policies by using [user-defined routes](#), and network filtering by using [network security groups](#). We recommend that all internet-facing resources also be protected by the [Azure DDoS Protection Standard](#).

Enterprises may need to connect their virtual datacenter to on-premises datacenters or other resources. This connectivity between Azure and on-premises networks is a crucial aspect when designing an effective architecture. Enterprises have two different ways to create this interconnection: transit over the Internet or via private direct

connections.

An [Azure Site-to-Site VPN](#) connects on-premises networks to your virtual datacenter in Azure. The link is established through secure encrypted connections (IPsec tunnels). Azure Site-to-Site VPN connections are flexible, quick to create, and typically don't require any additional hardware procurement. Based on industry standard protocols, most current network devices can create VPN connections to Azure over the internet or existing connectivity paths.

[ExpressRoute](#) enables private connections between your virtual datacenter and any on-premises networks. ExpressRoute connections don't go over the public Internet, and offer higher security, reliability, and higher speeds (up to 100 Gbps) along with consistent latency. ExpressRoute provides the benefits of compliance rules associated with private connections. With [ExpressRoute Direct](#), you can connect directly to Microsoft routers at either 10 Gbps or 100 Gbps.

Deploying ExpressRoute connections usually involves engaging with an ExpressRoute service provider (ExpressRoute Direct being the exception). For customers that need to start quickly, it's common to initially use Site-to-Site VPN to establish connectivity between a virtual datacenter and on-premises resources. Once your physical interconnection with your service provider is complete, then migrate connectivity over your ExpressRoute connection.

For large numbers of VPN or ExpressRoute connections, [Azure Virtual WAN](#) is a networking service that provides optimized and automated branch-to-branch connectivity through Azure. Virtual WAN lets you connect to and configure branch devices to communicate with Azure. Connecting and configuring can be done either manually or by using preferred provider devices through a Virtual WAN partner. Using preferred provider devices allows ease of use, simplification of connectivity, and configuration management. The Azure WAN built-in dashboard provides instant troubleshooting insights that can help save you time, and gives you an easy way to view large-scale site-to-site connectivity. Virtual WAN also provides security services with an optional Azure Firewall and Firewall Manager in your Virtual WAN hub.

## Connectivity within the cloud

[Azure Virtual Networks](#) and [virtual network peering](#) are the basic networking components in a virtual datacenter. A virtual network guarantees an isolation boundary for virtual datacenter resources. Peering allows intercommunication between different virtual networks within the same Azure region, across regions, and even between networks in different subscriptions. Both inside and between virtual networks, traffic flows can be controlled by sets of security rules specified for [network security groups](#), firewall policies ([Azure Firewall](#) or [network virtual appliances](#)), and custom [user-defined routes](#).

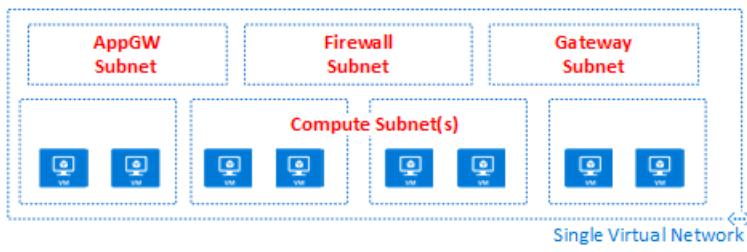
Virtual networks are also anchor points for integrating platform as a service (PaaS) Azure products like [Azure Storage](#), [Azure SQL](#), and other integrated public services that have public endpoints. With [service endpoints](#) and [Azure Private Link](#), you can integrate your public services with your private network. You can even take your public services private, but still enjoy the benefits of Azure-managed PaaS services.

# Virtual datacenter overview

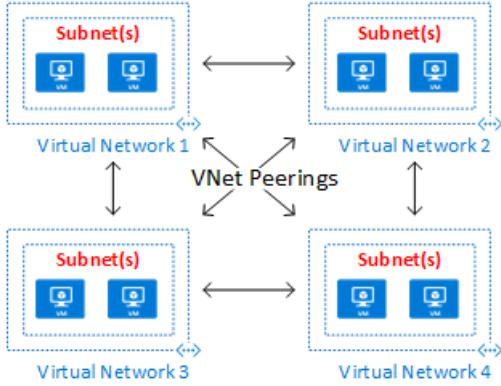
## Topologies

A virtual datacenter can be built using one of these high-level topologies, based on your needs and scale requirements:

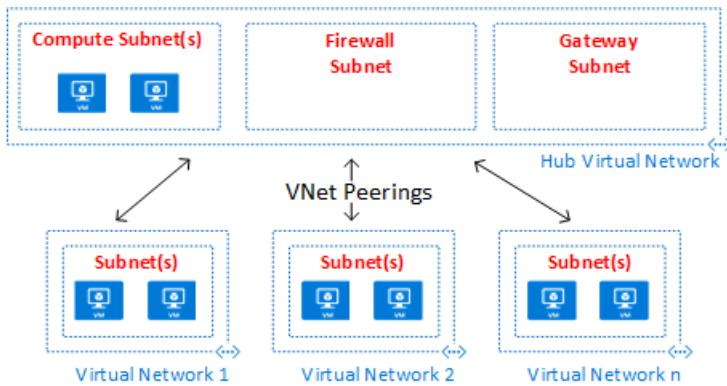
In a *Flat topology*, all resources are deployed in a single virtual network. Subnets allow for flow control and segregation.



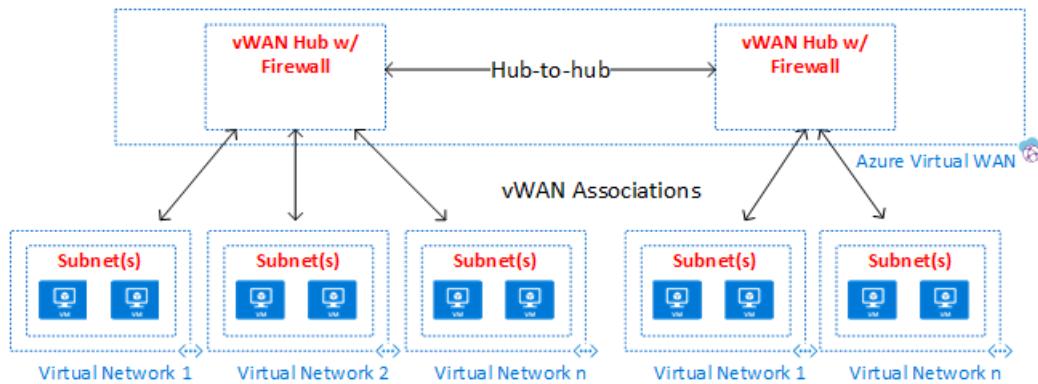
In a *Mesh topology*, virtual network peering connects all virtual networks directly to each other.



A *Peering hub and spoke topology* is well suited for distributed applications and teams with delegated responsibilities.



An *Azure Virtual WAN topology* can support large-scale branch office scenarios and global WAN services.



The peering hub and spoke topology and the Azure Virtual WAN topology both use a hub and spoke design, which is optimal for communication, shared resources, and centralized security policy. Hubs are built using either a virtual network peering hub (labeled as **Hub Virtual Network** in the diagram) or a Virtual WAN hub (labeled as **Azure Virtual WAN** in the diagram). Azure Virtual WAN is designed for large-scale branch-to-branch and branch-to-Azure communications, or for avoiding the complexities of building all the components individually in a virtual networking peering hub. In some cases, your requirements might mandate a virtual network peering hub design, such as the need for network virtual appliances in the hub.

In both of the hub and spoke topologies, the hub is the central network zone that controls and inspects all traffic between different zones: internet, on-premises, and the spokes. The hub and spoke topology helps the IT department centrally enforce security policies. It also reduces the potential for misconfiguration and exposure.

The hub often contains the common service components consumed by the spokes. The following examples are common central services:

- The Windows Active Directory infrastructure, required for user authentication of third parties that access from untrusted networks before they get access to the workloads in the spoke. It includes the related Active Directory Federation Services (AD FS).
- A Distributed Name System (DNS) service to resolve naming for the workload in the spokes, to access resources on-premises and on the internet if [Azure DNS](#) isn't used.
- A public key infrastructure (PKI), to implement single sign-on on workloads.
- Flow control of TCP and UDP traffic between the spoke network zones and the internet.
- Flow control between the spokes and on-premises.
- If needed, flow control between one spoke and another.

A virtual datacenter reduces overall cost by using the shared hub infrastructure between multiple spokes.

The role of each spoke can be to host different types of workloads. The spokes also provide a modular approach for repeatable deployments of the same workloads. Examples include dev/test, user acceptance testing, preproduction, and production. The spokes can also segregate and enable different groups within your organization. An example is DevOps groups. Inside a spoke, it's possible to deploy a basic workload or complex multitier workloads with traffic control between the tiers.

## Subscription limits and multiple hubs

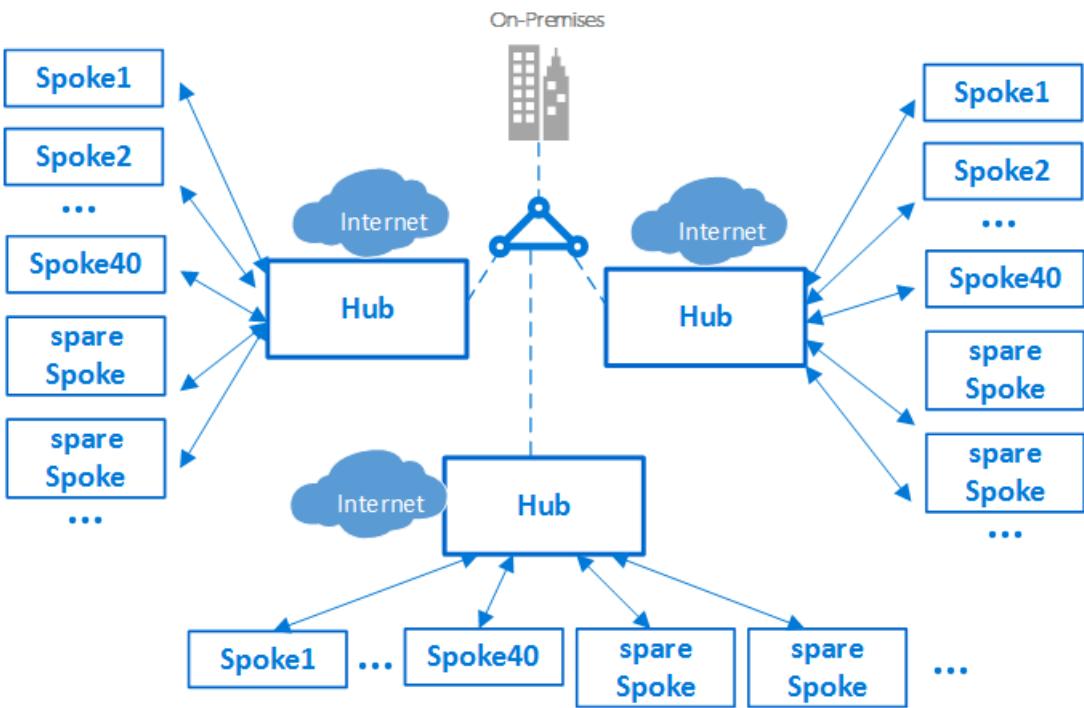
### IMPORTANT

Based on the size of your Azure deployments, a multiple hub strategy may be needed. When designing your hub and spoke strategy, ask "can this design scale to use another hub virtual network in this region?", also, "can this design scale to accommodate multiple regions?" It's far better to plan for a design that scales and not need it, than to fail to plan and need it.

When to scale to a secondary (or more) hub will depend on myriad factors, usually based on inherent limits on scale. Be sure to review the subscription, virtual network, and virtual machine [limits](#) when designing for scale.

In Azure, every component, whatever the type, is deployed in an Azure subscription. The isolation of Azure components in different Azure subscriptions can satisfy the requirements of different lines of business, such as setting up differentiated levels of access and authorization.

A single VDC implementation can scale up to large number of spokes, although, as with every IT system, there are platform limits. The hub deployment is bound to a specific Azure subscription, which has restrictions and limits (for example, a maximum number of virtual network peerings. For details, see [Azure subscription and service limits, quotas, and constraints](#)). In cases where limits may be an issue, the architecture can scale up further by extending the model from a single hub-spokes to a cluster of hub and spokes. Multiple hubs in one or more Azure regions can be connected using virtual network peering, ExpressRoute, Virtual WAN, or site-to-site VPN.

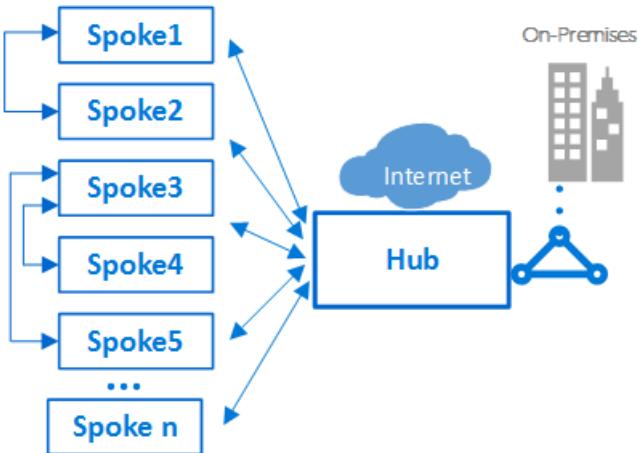


The introduction of multiple hubs increases the cost and management effort of the system. It is only justified due to scalability, system limits, redundancy, regional replication for end-user performance, or disaster recovery. In scenarios requiring multiple hubs, all the hubs should strive to offer the same set of services for operational ease.

### Interconnection between spokes

Inside a single spoke, or a flat network design, it's possible to implement complex multitier workloads. Multitier configurations can be implemented using subnets, one for every tier or application, in the same virtual network. Traffic control and filtering are done using network security groups and user-defined routes.

An architect might want to deploy a multitier workload across multiple virtual networks. With virtual network peering, spokes can connect to other spokes in the same hub or different hubs. A typical example of this scenario is the case where application processing servers are in one spoke, or virtual network. The database deploys in a different spoke, or virtual network. In this case, it's easy to interconnect the spokes with virtual network peering and, by doing that, avoid transiting through the hub. A careful architecture and security review should be done to ensure that bypassing the hub doesn't bypass important security or auditing points that might exist only in the hub.



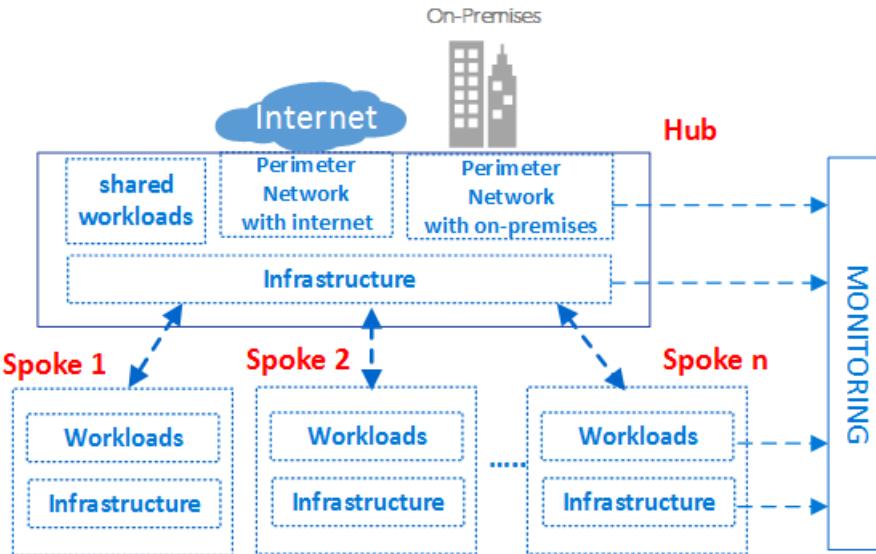
Spokes can also be interconnected to a spoke that acts as a hub. This approach creates a two-level hierarchy: the spoke in the higher level (level 0) becomes the hub of lower spokes (level 1) of the hierarchy. The spokes of a VDC implementation are required to forward the traffic to the central hub so that the traffic can transit to its destination in either the on-premises network or the public internet. An architecture with two levels of hubs introduces complex routing that removes the benefits of a simple hub-spoke relationship.

Although Azure allows complex topologies, one of the core principles of the VDC concept is repeatability and simplicity. To minimize management effort, the simple hub-spoke design is the VDC reference architecture that we recommend.

## Components

The virtual datacenter is made up of four basic component types: **Infrastructure**, **Perimeter Networks**, **Workloads**, and **Monitoring**.

Each component type consists of various Azure features and resources. Your VDC implementation is made up of instances of multiple components types and multiple variations of the same component type. For instance, you may have many different, logically separated workload instances that represent different applications. You use these different component types and instances to ultimately build the VDC.



The preceding high-level conceptual architecture of the VDC shows different component types used in different zones of the hub-spokes topology. The diagram shows infrastructure components in various parts of the architecture.

As good practice in general, access rights and privileges should be group-based. Dealing with groups rather than individual users eases maintenance of access policies, by providing a consistent way to manage it across teams, and aids in minimizing configuration errors. Assigning and removing users to and from appropriate groups helps keeping the privileges of a specific user up to date.

Each role group should have a unique prefix on their names. This prefix makes it easy to identify which group is associated with which workload. For example, a workload hosting an authentication service might have groups named **AuthServiceNetOps**, **AuthServiceSecOps**, **AuthServiceDevOps**, and **AuthServiceInfraOps**.

Centralized roles, or roles not related to a specific service, might be prefaced with **Corp**. An example is **CorpNetOps**.

Many organizations use a variation of the following groups to provide a major breakdown of roles:

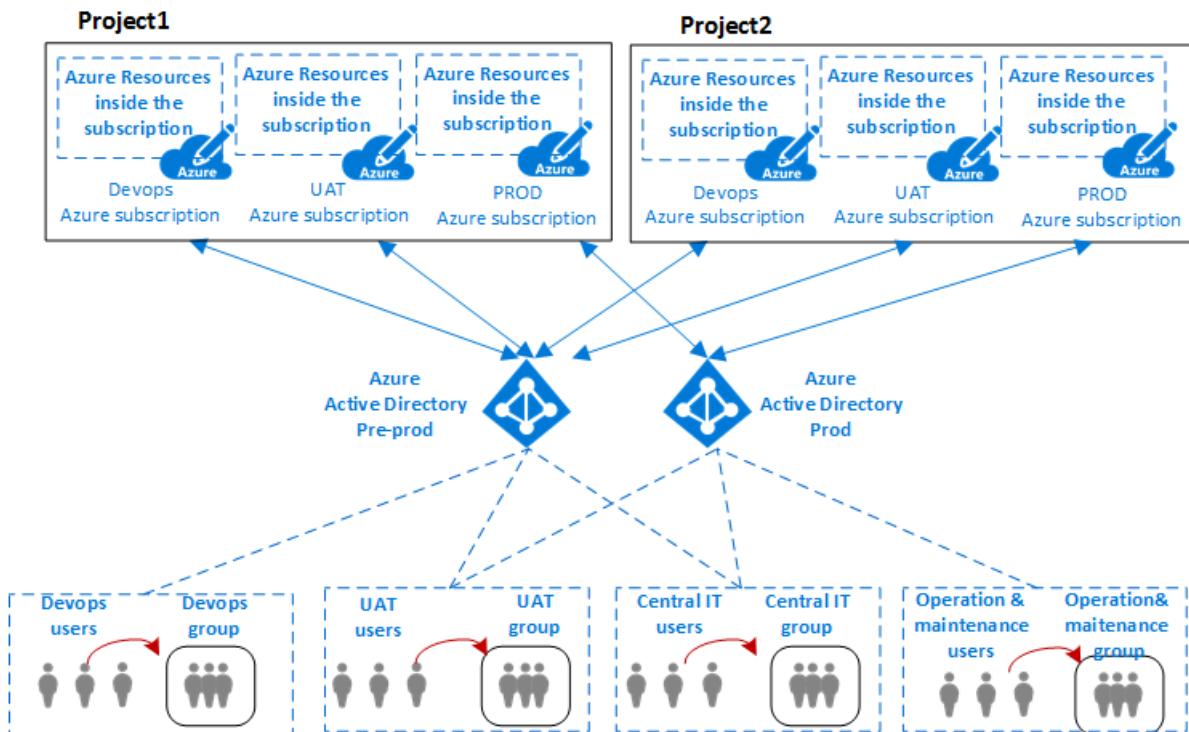
- The central IT team, **Corp**, has the ownership rights to control infrastructure components. Examples are networking and security. The group needs to have the role of contributor on the subscription, control of the hub, and network contributor rights in the spokes. Large organizations frequently split up these management responsibilities between multiple teams. Examples are a network operations **CorpNetOps** group with exclusive focus on networking and a security operations **CorpSecOps** group responsible for the firewall and security policy. In this specific case, two different groups need to be created for assignment of these custom roles.
- The dev/test group, **AppDevOps**, has the responsibility to deploy app or service workloads. This group takes the role of virtual machine contributor for IaaS deployments or one or more PaaS contributor's roles. For more information, see [Built-in roles for Azure resources](#). Optionally, the dev/test team might need visibility on security policies (network security groups) and routing policies (user-defined routes) inside the hub or a specific spoke.

In addition to the role of contributor for workloads, this group would also need the role of network reader.

- The operation and maintenance group, **CorpInfraOps** or **AppInfraOps**, has the responsibility of managing workloads in production. This group needs to be a subscription contributor on workloads in any production subscriptions. Some organizations might also evaluate if they need an additional escalation support team group with the role of subscription contributor in production and the central hub subscription. The additional group fixes potential configuration issues in the production environment.

The VDC is designed so that groups created for the central IT team, managing the hub, have corresponding groups at the workload level. In addition to managing hub resources only, the central IT team can control external access and top-level permissions on the subscription. Workload groups can also control resources and permissions of their virtual network independently from the central IT team.

The virtual datacenter is partitioned to securely host multiple projects across different lines of business. All projects require different isolated environments (dev, UAT, and production). Separate Azure subscriptions for each of these environments can provide natural isolation.



The preceding diagram shows the relationship between an organization's projects, users, and groups and the environments where the Azure components are deployed.

Typically in IT, an environment (or tier) is a system in which multiple applications are deployed and executed. Large enterprises use a development environment (where changes are made and tested) and a production environment (what end-users use). Those environments are separated, often with several staging environments in between them to allow phased deployment (rollout), testing, and rollback if problems arise. Deployment architectures vary significantly, but usually the basic process of starting at development (DEV) and ending at production (PROD) is still followed.

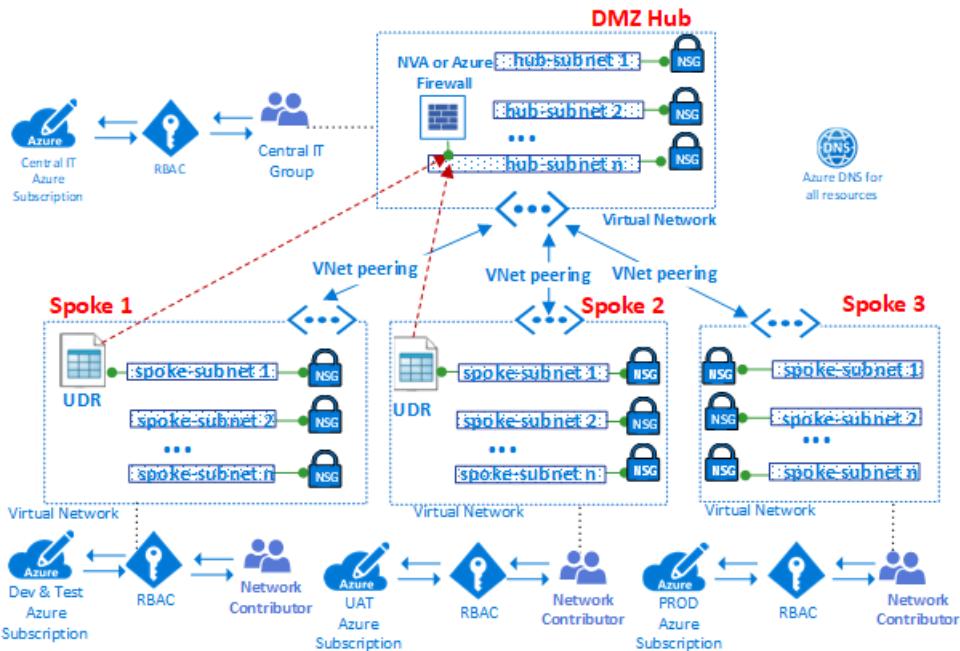
A common architecture for these types of mult-tier environments consists of DevOps for development and testing, UAT for staging, and production environments. Organizations can use single or multiple Azure AD tenants to define access and rights to these environments. The previous diagram shows a case where two different Azure AD tenants are used: one for DevOps and UAT, and the other exclusively for production.

The presence of different Azure AD tenants enforces the separation between environments. The same group of users, such as the central IT team, need to authenticate by using a different URI to access a different Azure AD tenant to modify the roles or permissions of either the DevOps or production environments of a project. The presence of different user authentications to access different environments reduces possible outages and other

issues caused by human errors.

#### Component type: Infrastructure

This component type is where most of the supporting infrastructure resides. It's also where your centralized IT, security, and compliance teams spend most of their time.



Infrastructure components provide an interconnection for the different components of a VDC implementation, and are present in both the hub and the spokes. The responsibility for managing and maintaining the infrastructure components is typically assigned to the central IT team or security team.

One of the primary tasks of the IT infrastructure team is to guarantee the consistency of IP address schemas across the enterprise. The private IP address space assigned to a VDC implementation must be consistent and NOT overlapping with private IP addresses assigned on your on-premises networks.

While NAT on the on-premises edge routers or in Azure environments can avoid IP address conflicts, it adds complications to your infrastructure components. Simplicity of management is one of the key goals of the VDC, so using NAT to handle IP concerns, while a valid solution, is not a recommended solution.

Infrastructure components have the following functionality:

- **Identity and directory services.** Access to every resource type in Azure is controlled by an identity stored in a directory service. The directory service stores not only the list of users, but also the access rights to resources in a specific Azure subscription. These services can exist cloud-only, or they can be synchronized with on-premises identity stored in Active Directory.
- **Virtual Network.** Virtual networks are one of main components of the VDC, and enable you to create a traffic isolation boundary on the Azure platform. A virtual network is composed of a single or multiple virtual network segments, each with a specific IP network prefix (a subnet, either IPv4 or dual stack IPv4/IPv6). The virtual network defines an internal perimeter area where IaaS virtual machines and PaaS services can establish private communications. VMs (and PaaS services) in one virtual network can't communicate directly to VMs (and PaaS services) in a different virtual network, even if both virtual networks are created by the same customer, under the same subscription. Isolation is a critical property that ensures customer VMs and communication remains private within a virtual network. Where cross-network connectivity is desired, the following features describe how that can be accomplished.
- **Virtual network peering.** The fundamental feature used to create the infrastructure of a VDC is virtual network peering, which connects two virtual networks in the same region, either through the Azure datacenter network or using the Azure worldwide backbone across regions.
- **Virtual Network service endpoints.** Service endpoints extend your virtual network private address space to

include your PaaS space. The endpoints also extend the identity of your virtual network to the Azure services over a direct connection. Endpoints allow you to secure your critical Azure service resources to only your virtual networks.

- **Private Link.** Azure Private Link enables you to access Azure PaaS Services (for example, [Azure Storage](#), [Azure Cosmos DB](#), and [Azure SQL Database](#)) and Azure hosted customer/partner services over a Private Endpoint in your virtual network. Traffic between your virtual network and the service traverses over the Microsoft backbone network, eliminating exposure from the public Internet. You can also create your own [Private Link Service](#) in your virtual network and deliver it privately to your customers. The setup and consumption experience using Azure Private Link is consistent across Azure PaaS, customer-owned, and shared partner services.
- **User-defined routes.** Traffic in a virtual network is routed by default based on the system routing table. A user-defined route is a custom routing table that network administrators can associate to one or more subnets to override the behavior of the system routing table and define a communication path within a virtual network. The presence of user-defined routes guarantees that egress traffic from the spoke transit through specific custom VMs or network virtual appliances and load balancers present in both the hub and the spokes.
- **Network security groups.** A network security group is a list of security rules that act as traffic filtering on IP sources, IP destinations, protocols, IP source ports, and IP destination ports (also called a Layer 4 five-tuple). The network security group can be applied to a subnet, a Virtual NIC associated with an Azure VM, or both. The network security groups are essential to implement a correct flow control in the hub and in the spokes. The level of security afforded by the network security group is a function of which ports you open, and for what purpose. Customers should apply additional per-VM filters with host-based firewalls such as iptables or the Windows Firewall.
- **DNS.** DNS provides name resolution for resources in a virtual datacenter. Azure provides DNS services for both [public](#) and [private](#) name resolution. Private zones provide name resolution both within a virtual network and across virtual networks. You can have private zones not only span across virtual networks in the same region, but also across regions and subscriptions. For public resolution, Azure DNS provides a hosting service for DNS domains, providing name resolution using Microsoft Azure infrastructure. By hosting your domains in Azure, you can manage your DNS records using the same credentials, APIs, tools, and billing as your other Azure services.
- **Management group, subscription, and resource group management.** A subscription defines a natural boundary to create multiple groups of resources in Azure. This separation can be for function, role segregation, or billing. Resources in a subscription are assembled together in logical containers known as resource groups. The resource group represents a logical group to organize the resources in a virtual datacenter. If your organization has many subscriptions, you may need a way to efficiently manage access, policies, and compliance for those subscriptions. Azure management groups provide a level of scope above subscriptions. You organize subscriptions into containers known as management groups and apply your governance conditions to the management groups. All subscriptions within a management group automatically inherit the conditions applied to the management group. To see these three features in a hierarchy view, see [Organizing your resources](#) in the Cloud Adoption Framework.
- **Role-based access control (RBAC).** RBAC can map organizational roles and rights to access specific Azure resources, allowing you to restrict users to only a certain subset of actions. If you're synchronizing Azure Active Directory with an on-premises Active Directory, you can use the same Active Directory groups in Azure that you use on-premises. With RBAC, you can grant access by assigning the appropriate role to users, groups, and applications within the relevant scope. The scope of a role assignment can be an Azure subscription, a resource group, or a single resource. RBAC allows inheritance of permissions. A role assigned at a parent scope also grants access to the children contained within it. Using RBAC, you can segregate duties and grant only the amount of access to users that they need to perform their jobs. For example, one employee can manage virtual machines in a subscription, while another can manage SQL Server databases in the same subscription.

#### **Component Type: Perimeter Networks**

Components of a perimeter network (sometimes called a DMZ network) connect your on-premises or physical datacenter networks, along with any internet connectivity. The perimeter typically requires a significant time

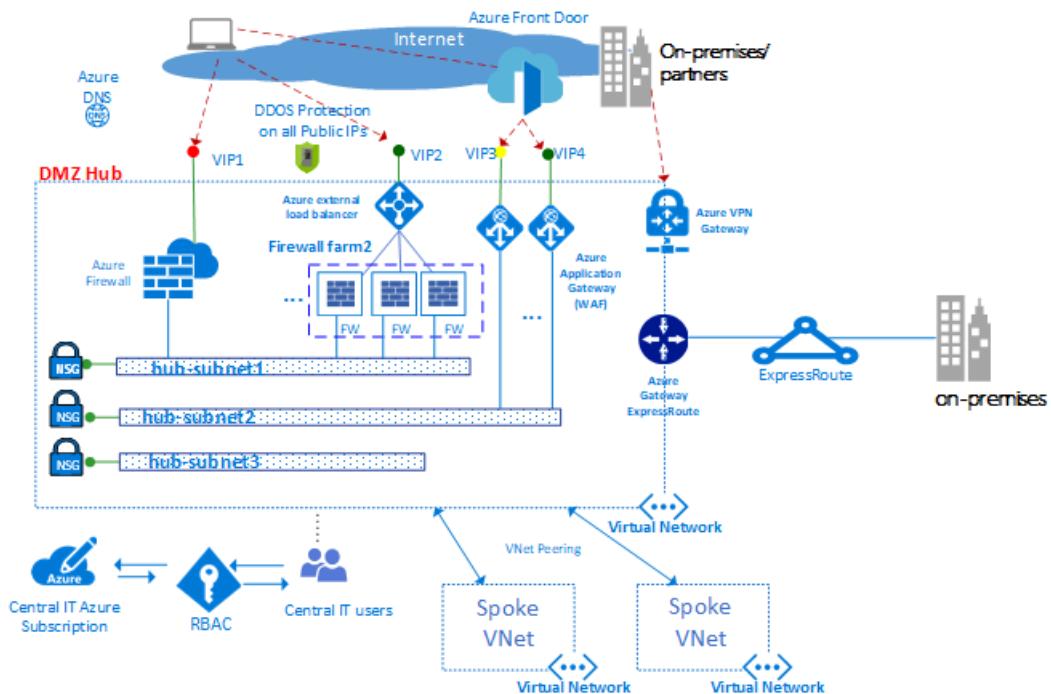
investment from your network and security teams.

Incoming packets should flow through the security appliances in the hub before reaching the back-end servers and services in the spokes. Examples include the firewall, IDS, and IPS. Before they leave the network, internet-bound packets from the workloads should also flow through the security appliances in the perimeter network. This flow enables policy enforcement, inspection, and auditing.

Perimeter network components include:

- Virtual networks, user-defined routes, and network security groups
- Network virtual appliances
- Azure Load Balancer
- Azure Application Gateway with web application firewall (WAF)
- Public IPs
- Azure Front Door with web application firewall (WAF)
- Azure Firewall and Azure Firewall Manager
- Standard DDoS Protection

Usually, the central IT team and security teams have responsibility for requirement definition and operation of the perimeter networks.



The preceding diagram shows the enforcement of two perimeters with access to the internet and an on-premises network, both resident in the DMZ hub. In the DMZ hub, the perimeter network to internet can scale up to support many lines of business, using multiple farms of Web Application Firewalls (WAFs) or Azure Firewalls. The hub also allows for on-premises connectivity via VPN or ExpressRoute as needed.

#### NOTE

In the preceding diagram, in the "DMZ Hub", many of the following features can be bundled together in an Azure Virtual WAN hub (such as virtual networks, user-defined routes, network security groups, VPN gateways, ExpressRoute gateways, Azure load balancers, Azure Firewalls, Firewall Manager, and DDOS). Using Azure Virtual WAN hubs can make the creation of the hub virtual network, and thus the VDC, much easier, since most of the engineering complexity is handled for you by Azure when you deploy an Azure Virtual WAN hub.

**Virtual networks.** The hub is typically built on a virtual network with multiple subnets to host the different types of

services that filter and inspect traffic to or from the internet via Azure Firewall, NVAs, WAF, and Azure Application Gateway instances.

**User-defined routes** Using user-defined routes, customers can deploy firewalls, IDS/IPS, and other virtual appliances, and route network traffic through these security appliances for security boundary policy enforcement, auditing, and inspection. User-defined routes can be created in both the hub and the spokes to guarantee that traffic transits through the specific custom VMs, Network Virtual Appliances, and load balancers used by a VDC implementation. To guarantee that traffic generated from virtual machines residing in the spoke transits to the correct virtual appliances, a user-defined route needs to be set in the subnets of the spoke by setting the front-end IP address of the internal load balancer as the next hop. The internal load balancer distributes the internal traffic to the virtual appliances (load balancer back-end pool).

**Azure Firewall** is a managed network security service that protects your Azure Virtual Network resources. It's a stateful managed firewall with high availability and cloud scalability. You can centrally create, enforce, and log application and network connectivity policies across subscriptions and virtual networks. Azure Firewall uses a static public IP address for your virtual network resources. It allows outside firewalls to identify traffic that originates from your virtual network. The service is fully integrated with Azure Monitor for logging and analytics.

If you use the Azure Virtual WAN topology, the [Azure Firewall Manager](#) is a security management service that provides central security policy and route management for cloud-based security perimeters. It works with Azure Virtual WAN hub, a Microsoft-managed resource that lets you easily create hub and spoke architectures. When security and routing policies are associated with such a hub, it's referred to as a secured virtual hub.

**Network virtual appliances.** In the hub, the perimeter network with access to the internet is normally managed through an Azure Firewall instance or a farm of firewalls or web application firewall (WAF).

Different lines of business commonly use many web applications, which tend to suffer from various vulnerabilities and potential exploits. Web application firewalls are a special type of product used to detect attacks against web applications, HTTP/HTTPS, in more depth than a generic firewall. Compared with tradition firewall technology, WAFs have a set of specific features to protect internal web servers from threats.

An Azure Firewall or NVA firewall both use a common administration plane, with a set of security rules to protect the workloads hosted in the spokes, and control access to on-premises networks. The Azure Firewall has scalability built in, whereas NVA firewalls can be manually scaled behind a load balancer. Generally, a firewall farm has less specialized software compared with a WAF, but has a broader application scope to filter and inspect any type of traffic in egress and ingress. If an NVA approach is used, they can be found and deployed from Azure Marketplace.

We recommend that you use one set of Azure Firewall instances, or NVAs, for traffic originating on the internet. Use another for traffic originating on-premises. Using only one set of firewalls for both is a security risk as it provides no security perimeter between the two sets of network traffic. Using separate firewall layers reduces the complexity of checking security rules and makes it clear which rules correspond to which incoming network request.

**Azure Load Balancer** offers a high availability Layer 4 (TCP/UDP) service, which can distribute incoming traffic among service instances defined in a load-balanced set. Traffic sent to the load balancer from front-end endpoints (public IP endpoints or private IP endpoints) can be redistributed with or without address translation to a set of back-end IP address pool (such as network virtual appliances or virtual machines).

Azure Load Balancer can probe the health of the various server instances as well, and when an instance fails to respond to a probe, the load balancer stops sending traffic to the unhealthy instance. In a virtual datacenter, an external load balancer is deployed to the hub and the spokes. In the hub, the load balancer is used to efficiently route traffic across firewall instances, and in the spokes, load balancers are used to manage application traffic.

**Azure Front Door** (AFD) is Microsoft's highly available and scalable Web Application Acceleration Platform, Global HTTP Load Balancer, Application Protection, and Content Delivery Network. Running in more than 100 locations at the edge of Microsoft's Global Network, AFD enables you to build, operate, and scale out your dynamic web

application and static content. AFD provides your application with world-class end-user performance, unified regional/stamp maintenance automation, BCDR automation, unified client/user information, caching, and service insights. The platform offers:

- Performance, reliability, and support service-level agreements (SLAs).
- Compliance certifications.
- Auditable security practices that are developed, operated, and natively supported by Azure.

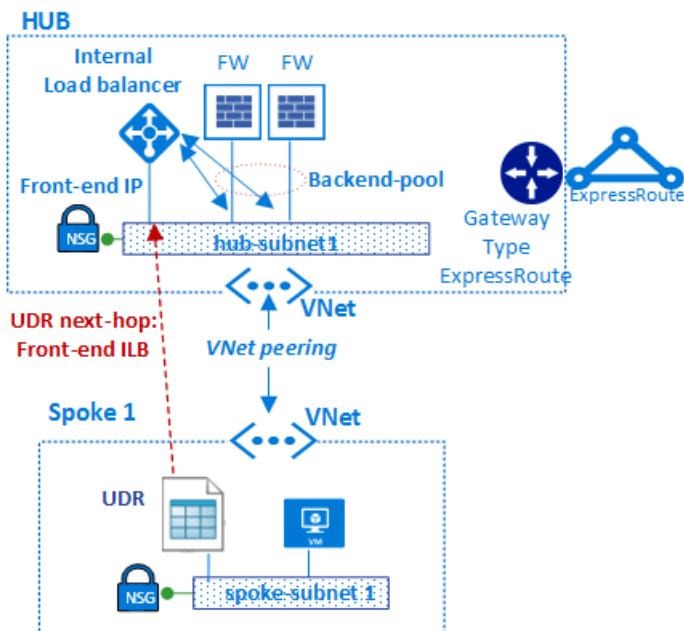
Azure Front Door also provides a web application firewall (WAF), which protects web applications from common vulnerabilities and exploits.

[Azure Application Gateway](#) is a dedicated virtual appliance providing a managed application delivery controller. It offers various Layer 7 load-balancing capabilities for your application. It allows you to optimize web farm performance by offloading CPU-intensive SSL termination to the application gateway. It also provides other Layer 7 routing capabilities, such as round-robin distribution of incoming traffic, cookie-based session affinity, URL-path-based routing, and the ability to host multiple websites behind a single application gateway. A web application firewall (WAF) is also provided as part of the application gateway WAF SKU. This SKU provides protection to web applications from common web vulnerabilities and exploits. Application Gateway can be configured as internet facing gateway, internal only gateway, or a combination of both.

[Public IPs](#). With some Azure features, you can associate service endpoints to a public IP address so that your resource is accessible from the internet. This endpoint uses NAT to route traffic to the internal address and port on the virtual network in Azure. This path is the primary way for external traffic to pass into the virtual network. You can configure public IP addresses to determine which traffic is passed in and how and where it's translated onto the virtual network.

[Azure DDoS Protection Standard](#) provides additional mitigation capabilities over the [Basic service](#) tier that are tuned specifically to Azure Virtual Network resources. DDoS Protection Standard is simple to enable and requires no application changes. Protection policies are tuned through dedicated traffic monitoring and machine learning algorithms. Policies are applied to public IP addresses associated to resources deployed in virtual networks. Examples include Azure Load Balancer, Azure Application Gateway, and Azure Service Fabric instances. Near real-time, system-generated logs are available through Azure Monitor views during an attack and for history. Application layer protection can be added through the Azure Application Gateway web application firewall. Protection is provided for IPv4 and IPv6 Azure public IP addresses.

The hub and spoke topology uses virtual network peering and user-defined routes to route traffic properly.



In the diagram, the user-defined route ensures that traffic flows from the spoke to the firewall before passing to on-premises through the ExpressRoute gateway (if the firewall policy allows that flow).

#### Component type: Monitoring

[Monitoring components](#) provide visibility and alerting from all the other component types. All teams should have

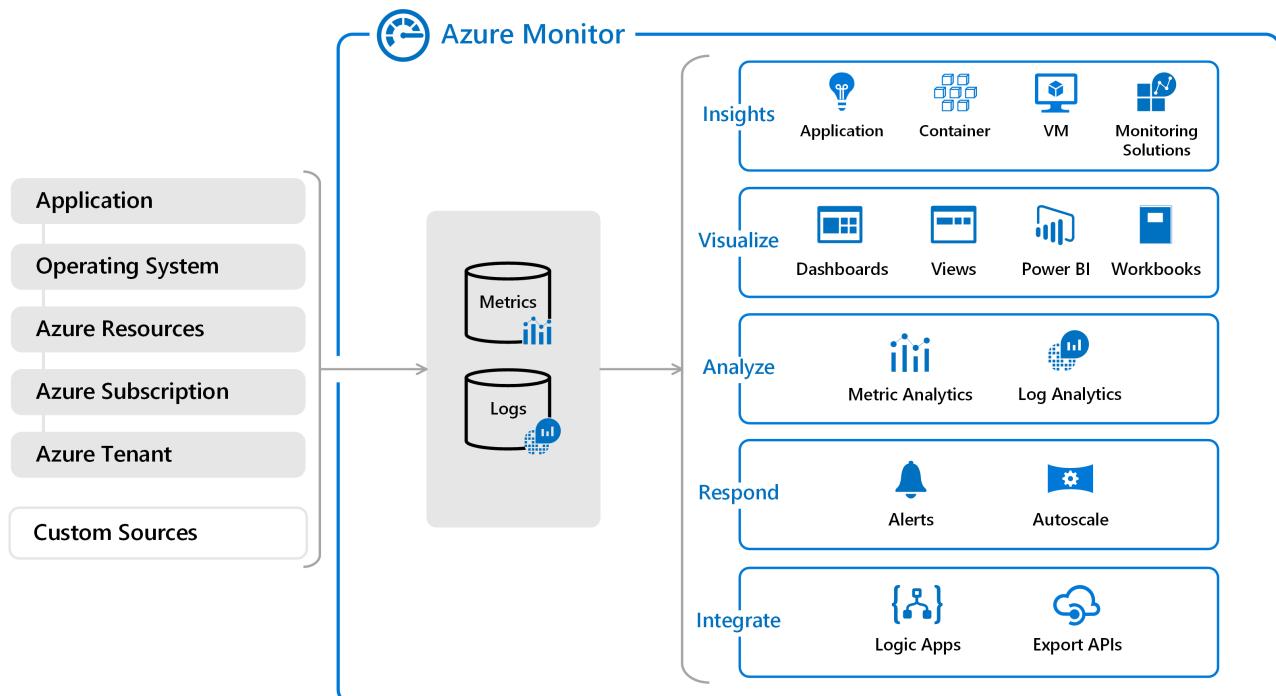
access to monitoring for the components and services they have access to. If you have a centralized help desk or operations teams, they require integrated access to the data provided by these components.

Azure offers different types of logging and monitoring services to track the behavior of Azure-hosted resources. Governance and control of workloads in Azure is based not just on collecting log data but also on the ability to trigger actions based on specific reported events.

**Azure Monitor.** Azure includes multiple services that individually perform a specific role or task in the monitoring space. Together, these services deliver a comprehensive solution for collecting, analyzing, and acting on system-generated logs from your applications and the Azure resources that support them. They can also work to monitor critical on-premises resources in order to provide a hybrid monitoring environment. Understanding the tools and data that are available is the first step in developing a complete monitoring strategy for your applications.

There are two fundamental types of logs in Azure Monitor:

- **Metrics** are numerical values that describe some aspect of a system at a particular point in time. They are lightweight and capable of supporting near real-time scenarios. For many Azure resources, you'll see data collected by Azure Monitor right in their Overview page in the Azure portal. As an example, look at any virtual machine and you'll see several charts displaying performance metrics. Select any of the graphs to open the data in metrics explorer in the Azure portal, which allows you to chart the values of multiple metrics over time. You can view the charts interactively or pin them to a dashboard to view them with other visualizations.
- **Logs** contain different kinds of data organized into records with different sets of properties for each type. Events and traces are stored as logs along with performance data, which can all be combined for analysis. Log data collected by Azure Monitor can be analyzed with queries to quickly retrieve, consolidate, and analyze collected data. Logs are stored and queried from [Log Analytics](#). You can create and test queries using Log Analytics in the Azure portal and then either directly analyze the data using these tools or save queries for use with visualizations or alert rules.



Azure Monitor can collect data from a variety of sources. You can think of monitoring data for your applications in tiers ranging from your application, any operating system, and the services it relies on, down to the Azure platform itself. Azure Monitor collects data from each of the following tiers:

- **Application monitoring data:** Data about the performance and functionality of the code you have written, regardless of its platform.
- **Guest OS monitoring data:** Data about the operating system on which your application is running. This OS

could be running in Azure, another cloud, or on-premises.

- **Azure resource monitoring data:** Data about the operation of an Azure resource.
- **Azure subscription monitoring data:** Data about the operation and management of an Azure subscription, as well as data about the health and operation of Azure itself.
- **Azure tenant monitoring data:** Data about the operation of tenant-level Azure services, such as Azure Active Directory.
- **Custom sources:** Logs sent from on-premises sources can be included as well. Examples include on-premises server events or network device syslog output.

Monitoring data is only useful if it can increase your visibility into the operation of your computing environment. Azure Monitor includes several features and tools that provide valuable insights into your applications and other resources that they depend on. Monitoring solutions and features such as Application Insights and Azure Monitor for containers provide deep insights into different aspects of your application and specific Azure services.

Monitoring solutions in Azure Monitor are packaged sets of logic that provide insights for a particular application or service. They include logic for collecting monitoring data for the application or service, queries to analyze that data, and views for visualization. Monitoring solutions are available from Microsoft and partners to provide monitoring for various Azure services and other applications.

With all of this rich data collected, it's important to take proactive action on events happening in your environment where manual queries alone won't suffice. Alerts in Azure Monitor proactively notify you of critical conditions and potentially attempt to take corrective action. Alert rules based on metrics provide near real-time alerting based on numeric values, while rules based on logs allow for complex logic across data from multiple sources. Alert rules in Azure Monitor use action groups, which contain unique sets of recipients and actions that can be shared across multiple rules. Based on your requirements, action groups can perform such actions as using webhooks that cause alerts to start external actions or to integrate with your ITSM tools.

Azure Monitor also allows the creation of custom dashboards. Azure dashboards allow you to combine different kinds of data, including both metrics and logs, into a single pane in the Azure portal. You can optionally share the dashboard with other Azure users. Elements throughout Azure Monitor can be added to an Azure dashboard in addition to the output of any log query or metrics chart. For example, you could create a dashboard that combines tiles that show a graph of metrics, a table of activity logs, a usage chart from Application Insights, and the output of a log query.

Finally, Azure Monitor data is a native source for Power BI. Power BI is a business analytics service that provides interactive visualizations across a variety of data sources and is an effective means of making data available to others within and outside your organization. You can configure Power BI to automatically import log data from Azure Monitor to take advantage of these additional visualizations.

[Azure Network Watcher](#) provides tools to monitor, diagnose, and view metrics and enable or disable logs for resources in a virtual network in Azure. It's a multifaceted service that allows the following functionalities and more:

- Monitor communication between a virtual machine and an endpoint.
- View resources in a virtual network and their relationships.
- Diagnose network traffic filtering problems to or from a VM.
- Diagnose network routing problems from a VM.
- Diagnose outbound connections from a VM.
- Capture packets to and from a VM.
- Diagnose problems with a virtual network gateway and connections.
- Determine relative latencies between Azure regions and internet service providers.
- View security rules for a network interface.
- View network metrics.

- Analyze traffic to or from a network security group.
- View diagnostic logs for network resources.

#### **Component type: Workloads**

Workload components are where your actual applications and services reside. It's where your application development teams spend most of their time.

The workload possibilities are endless. The following are just a few of the possible workload types:

**Internal applications:** Line-of-business applications are critical to enterprise operations. These applications have some common characteristics:

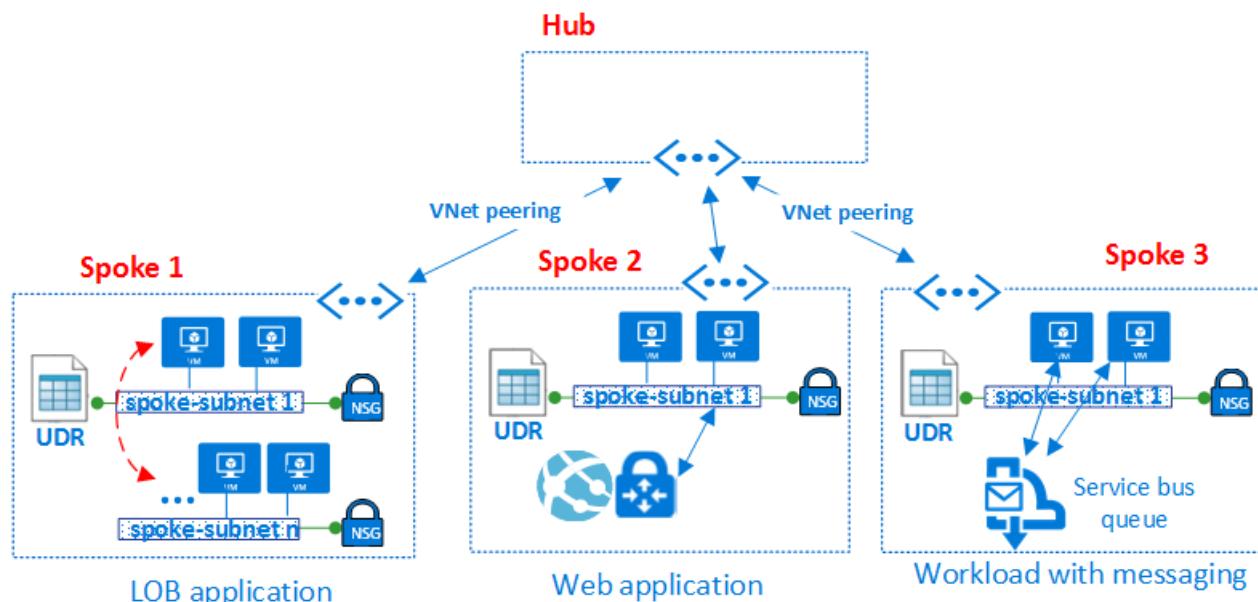
- **Interactive:** Data is entered, and results or reports are returned.
- **Data-driven:** Data intensive with frequent access to databases or other storage.
- **Integrated:** Offer integration with other systems within or outside the organization.

**Customer-facing web sites (internet-facing or internally facing):** Most internet applications are web sites. Azure can run a web site via either an IaaS virtual machine or an [Azure Web Apps](#) site (PaaS). Azure Web Apps integrates with virtual networks to deploy web apps in a spoke network zone. Internally facing web sites don't need to expose a public internet endpoint because the resources are accessible via private non-internet routable addresses from the private virtual network.

**Big data analytics:** When data needs to scale up to larger volumes, relational databases may not perform well under the extreme load or unstructured nature of the data. [Azure HDInsight](#) is a managed, full-spectrum, open-source analytics service in the cloud for enterprises. You can use open-source frameworks such as Hadoop, Apache Spark, Apache Hive, LLAP, Apache Kafka, Apache Storm, and R. HDInsight supports deploying into a location-based virtual network, can be deployed to a cluster in a spoke of the virtual datacenter.

**Events and Messaging:** [Azure Event Hubs](#) is a big data streaming platform and event ingestion service. It can receive and process millions of events per second. It provides low latency and configurable time retention, enabling you to ingest massive amounts of data into Azure and read it from multiple applications. A single stream can support both real-time and batch-based pipelines.

You can implement a highly reliable cloud messaging service between applications and services through [Azure Service Bus](#). It offers asynchronous brokered messaging between client and server, structured first-in-first-out (FIFO) messaging, and publishes and subscribe capabilities.



These examples barely scratch the surface of the types of workloads you can create in Azure—everything from a basic Web and SQL app to the latest in IoT, big data, machine learning, AI, and so much more.

## **Highly availability: multiple virtual datacenters**

So far, this article has focused on the design of a single VDC, describing the basic components and architectures that contribute to resiliency. Azure features such as Azure load balancer, NVAs, availability zones, availability sets, scale sets, and other capabilities that help you include solid SLA levels into your production services.

However, because a virtual datacenter is typically implemented within a single region, it might be vulnerable to outages that affect the entire region. Customers that require high availability must protect the services through deployments of the same project in two or more VDC implementations deployed to different regions.

In addition to SLA concerns, several common scenarios benefit from running multiple virtual datacenters:

- Regional or global presence of your end users or partners.
- Disaster recovery requirements.
- A mechanism to divert traffic between datacenters for load or performance.

### **Regional/global presence**

Azure datacenters exist in many regions worldwide. When selecting multiple Azure datacenters, consider two related factors: geographical distances and latency. To optimize user experience, evaluate the distance between each virtual datacenter as well as the distance from each virtual datacenter to the end users.

An Azure region that hosts your virtual datacenter must conform with regulatory requirements of any legal jurisdiction under which your organization operates.

### **Disaster recovery**

The design of a disaster recovery plan depends on the types of workloads and the ability to synchronize state of those workloads between different VDC implementations. Ideally, most customers desire a fast fail-over mechanism, and this requirement may need application data synchronization between deployments running in multiple VDC implementations. However, when designing disaster recovery plans, it's important to consider that most applications are sensitive to the latency that can be caused by this data synchronization.

Synchronization and heartbeat monitoring of applications in different VDC implementations requires them to communicate over the network. Multiple VDC implementations in different regions can be connected through:

- Hub-to-hub communication built into Azure Virtual WAN hubs across regions in the same Virtual WAN.
- Virtual network peering to connect hubs across regions.
- ExpressRoute private peering, when the hubs in each VDC implementation are connected to the same ExpressRoute circuit.
- Multiple ExpressRoute circuits connected via your corporate backbone, and your multiple VDC implementations connected to the ExpressRoute circuits.
- Site-to-site VPN connections between the hub zone of your VDC implementations in each Azure region.

Typically, Virtual WAN hubs, virtual network peering, or ExpressRoute connections are preferred for network connectivity, due to the higher bandwidth and consistent latency levels when passing through the Microsoft backbone.

Run network qualification tests to verify the latency and bandwidth of these connections, and decide whether synchronous or asynchronous data replication is appropriate based on the result. It's also important to weigh these results in view of the optimal recovery time objective (RTO).

### **Disaster recovery: diverting traffic from one region to another**

Both [Azure Traffic Manager](#) and [Azure Front Door](#) periodically check the service health of listening endpoints in different VDC implementations and, if those endpoints fail, route automatically to the next closest VDC. Traffic Manager uses real-time user measurements and DNS to route users to the closest (or next closest during failure). Azure Front Door is a reverse proxy at over 100 Microsoft backbone edge sites, using anycast to route users to the closest listening endpoint.

## **Summary**

A virtual datacenter approach to datacenter migration creates a scalable architecture that optimizes Azure resource use, lowers costs, and simplifies system governance. The virtual datacenter is typically based on hub and spoke network topologies (using either virtual network peering or Virtual WAN hubs). Common shared services provided in the hub, and specific applications and workloads are deployed in the spokes. The virtual datacenter also matches the structure of company roles, where different departments such as Central IT, DevOps, and Operations and Maintenance all work together while performing their specific roles. The virtual datacenter supports migrating existing on-premises workloads to Azure, but also provides many advantages to cloud-native deployments.

## References

Learn more about the Azure capabilities discussed in this document.

### Network features

[Azure Virtual Networks](#)

[Network Security Groups](#)

[Service Endpoints](#)

[Private Link](#)

[User-Defined Routes](#)

[Network Virtual Appliances](#)

[Public IP Addresses](#)

[Azure DNS](#)

### Load balancing

[Azure Front Door](#)

[Azure Load Balancer \(L4\)](#)

[Application Gateway \(L7\)](#)

[Azure Traffic Manager](#)

### Connectivity

[Virtual Network Peering](#)

[Virtual Private Network](#)

[Virtual WAN](#)

[ExpressRoute](#)

[ExpressRoute Direct](#)

### Identity

[Azure Active Directory](#)

[Multi-Factor Authentication](#)

[Role-Based Access Control](#)

[Default Azure AD Roles](#)

### Monitoring

[Network Watcher](#)

[Azure Monitor](#)

[Log Analytics](#)

### Best practices

[Management Group](#)

[Subscription Management](#)

[Resource Group Management](#)

[Azure Subscription Limits](#)

### Security

[Azure Firewall](#)

[Firewall Manager](#)

[Application Gateway WAF](#)

[Front Door WAF](#)

[Azure DDoS](#)

#### Other Azure services

[Azure Storage](#)

[Azure SQL](#)

[Azure Web Apps](#)

[Azure Cosmos DB](#)

[HDInsight](#)

[Event Hubs](#)

[Service Bus](#)

[Azure IoT](#)

[Azure Machine Learning](#)

## Next steps

- Learn more about [virtual network peering](#), the core technology of hub and spoke topologies.
- Implement [Azure Active Directory](#) to use [role-based access control](#).
- Develop a subscription and resource management model using role-based access control that fits the structure, requirements, and policies of your organization. The most important activity is planning. Analyze how reorganizations, mergers, new product lines, and other considerations will affect your initial models to ensure you can scale to meet future needs and growth.

# Perimeter networks

11/9/2020 • 6 minutes to read • [Edit Online](#)

Perimeter networks enable secure connectivity between your cloud networks and your on-premises or physical datacenter networks, along with any connectivity to and from the internet. A perimeter network is sometimes called a demilitarized zone or DMZ.

For perimeter networks to be effective, incoming packets must flow through security appliances hosted in secure subnets before reaching back-end servers. Examples include the firewall, intrusion detection systems, and intrusion prevention systems. Before they leave the network, internet-bound packets from workloads should also flow through the security appliances in the perimeter network. The purposes of this flow are policy enforcement, inspection, and auditing.

Perimeter networks make use of the following Azure features and services:

- [Virtual networks, user-defined routes](#), and [network security groups](#)
- [Network virtual appliances \(NVAs\)](#)
- [Azure Load Balancer](#)
- [Azure Application Gateway](#) and [Web Application Firewall \(WAF\)](#)
- [Public IPs](#)
- [Azure Front Door with Web Application Firewall](#)
- [Azure Firewall](#)

## NOTE

Azure reference architectures provide example templates that you can use to implement your own perimeter networks:

- [Implement a perimeter network between Azure and your on-premises datacenter](#)
- [Implement a perimeter network between Azure and the internet](#)

Usually, your Central IT team and security teams are responsible for defining requirements for operating your perimeter networks.

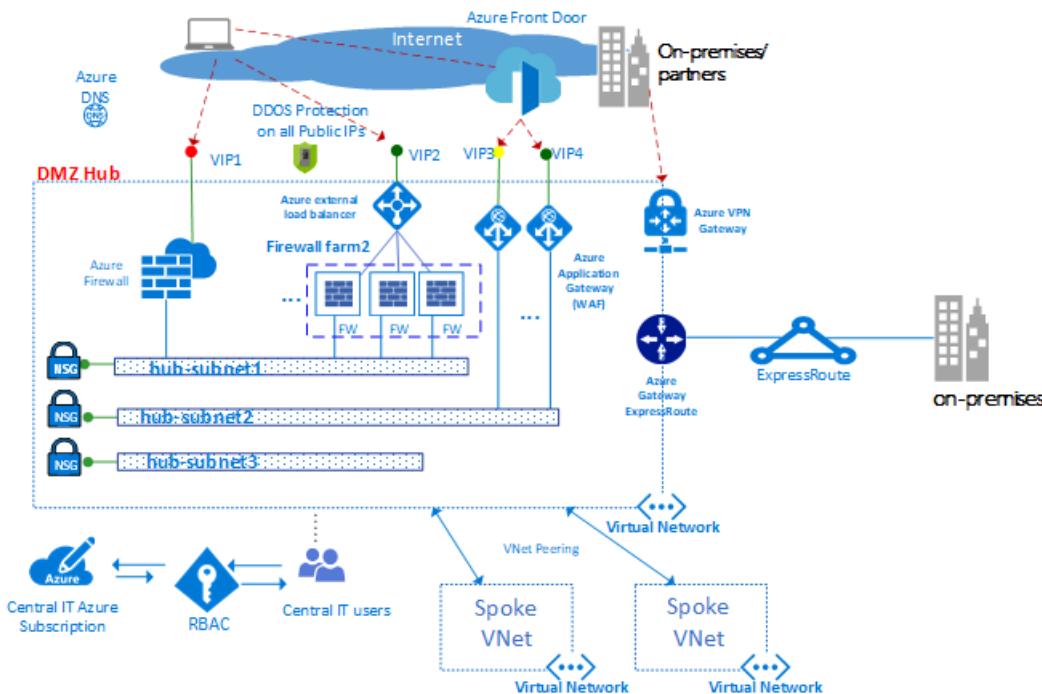


Figure 1: Example

of a hub and spoke network topology.

The diagram above shows an example [hub and spoke network topology](#) that implements enforcement of two perimeters with access to the internet and an on-premises network. Both perimeters reside in the DMZ hub. In the DMZ hub, the perimeter network to the internet can scale up to support many lines of business via multiple farms of WAFs and Azure Firewall instances that help protect the spoke virtual networks. The hub also allows for connectivity via VPN or Azure ExpressRoute as needed.

## Virtual networks

Perimeter networks are typically built using a [virtual network](#) with multiple subnets to host the different types of services that filter and inspect traffic to or from the internet via NVAs, WAFs, and Azure Application Gateway instances.

## User-defined routes

By using [user-defined routes](#), customers can deploy firewalls, intrusion detection systems, intrusion prevention systems, and other virtual appliances. Customers can then route network traffic through these security appliances for security boundary policy enforcement, auditing, and inspection. User-defined routes can be created to guarantee that traffic passes through the specified custom VMs, NVAs, and load balancers.

In a hub and spoke network example, guaranteeing that traffic generated by virtual machines that reside in the spoke passes through the correct virtual appliances in the hub requires a user-defined route defined in the subnets of the spoke. This route sets the front-end IP address of the internal load balancer as the next hop. The internal load balancer distributes the internal traffic to the virtual appliances (load balancer back-end pool).

## Azure Firewall

[Azure Firewall](#) is a managed cloud-based service that helps protect your Azure Virtual Network resources. It's a fully stateful managed firewall with built-in high availability and unrestricted cloud scalability. You can centrally create, enforce, and log application and network connectivity policies across subscriptions and virtual networks.

Azure Firewall uses a static public IP address for your virtual network resources. It allows outside firewalls to identify traffic that originates from your virtual network. The service interoperates with Azure Monitor for logging and analytics.

## Network virtual appliances

Perimeter networks with access to the internet are typically managed through an Azure Firewall instance or a farm of firewalls or [web application firewalls](#).

Different lines of business commonly use many web applications. These applications tend to suffer from various vulnerabilities and potential exploits. A Web Application Firewall detects attacks against web applications (HTTP/S) in more depth than a generic firewall. Compared with tradition firewall technology, web application firewalls have a set of specific features to help protect internal web servers from threats.

An Azure Firewall instance and a [network virtual appliance][NVA] firewall use a common administration plane with a set of security rules to help protect the workloads hosted in the spokes and control access to on-premises networks. Azure Firewall has built-in scalability, whereas NVA firewalls can be manually scaled behind a load balancer.

A firewall farm typically has less specialized software compared with a WAF, but it has a broader application scope to filter and inspect any type of traffic in egress and ingress. If you use an NVA approach, you can find and deploy the software from the Azure Marketplace.

Use one set of Azure Firewall instances (or NVAs) for traffic that originates on the internet and another set for traffic that originates on-premises. Using only one set of firewalls for both is a security risk because it provides no security perimeter between the two sets of network traffic. Using separate firewall layers reduces the complexity of checking security rules and makes clear which rules correspond to which incoming network requests.

## Azure Load Balancer

[Azure Load Balancer](#) offers a high-availability Layer 4 (TCP/UDP) service, which can distribute incoming traffic among service instances defined in a load-balanced set. Traffic sent to the load balancer from front-end endpoints (public IP endpoints or private IP endpoints) can be redistributed with or without address translation to a pool of back-end IP addresses (such as NVAs or VMs).

Azure Load Balancer can also probe the health of the various server instances. When an instance fails to respond to a probe, the load balancer stops sending traffic to the unhealthy instance.

As an example of using a hub and spoke network topology, you can deploy an external load balancer to both the hub and the spokes. In the hub, the load balancer efficiently routes traffic to services in the spokes. In the spokes, load balancers manage application traffic.

## Azure Front Door

[Azure Front Door](#) is Microsoft's highly available and scalable web application acceleration platform and global HTTPS load balancer. You can use Azure Front Door to build, operate, and scale out your dynamic web application and static content. It runs in more than 100 locations at the edge of Microsoft's global network.

Azure Front Door provides your application with unified regional/stamp maintenance automation, BCDR automation, unified client/user information, caching, and service insights. The platform offers performance, reliability, and support SLAs. It also offers compliance certifications and auditable security practices that are developed, operated, and supported natively by Azure.

## Azure Application Gateway

[Azure Application Gateway](#) is a dedicated virtual appliance that provides a managed application delivery controller. It offers various Layer 7 load-balancing capabilities for your application.

Azure Application Gateway allows you to optimize web farm productivity by offloading CPU-intensive SSL termination to the application gateway. It also provides other Layer 7 routing capabilities, including round-robin

distribution of incoming traffic, cookie-based session affinity, URL path-based routing, and the ability to host multiple websites behind a single application gateway.

The Azure Application Gateway WAF SKU includes a Web Application Firewall. This SKU provides protection to web applications from common web vulnerabilities and exploits. You can configure Azure Application Gateway as an internet-facing gateway, an internal-only gateway, or a combination of both.

## Public IPs

With some Azure features, you can associate service endpoints to a [public IP](#) address so that your resource can be accessed from the internet. This endpoint uses network address translation (NAT) to route traffic to the internal address and port on the Azure Virtual Network. This path is the primary way for external traffic to pass into the virtual network. You can configure public IP addresses to determine what traffic is passed in, and how and where it's translated onto the virtual network.

## Azure DDoS Protection Standard

[Azure DDoS Protection Standard](#) provides additional mitigation capabilities over the [basic service](#) tier that are tuned specifically to Azure Virtual Network resources. DDoS protection standard is simple to enable and requires no application changes.

You can tune protection policies through dedicated traffic monitoring and machine-learning algorithms. Policies are applied to public IP addresses associated to resources deployed in virtual networks. Examples include Azure Load Balancer, Application Gateway, and Service Fabric instances.

Real-time telemetry is available through Azure Monitor views both during an attack and for historical purposes. You can add application-layer protection by using the Web Application Firewall in Azure Application Gateway. Protection is provided for IPv4 Azure public IP addresses.

# Hub and spoke network topology

11/9/2020 • 5 minutes to read • [Edit Online](#)

*Hub and spoke* is a networking model for efficiently managing common communication or security requirements. It also helps avoid Azure subscription limitations. This model addresses the following concerns:

- **Cost savings and management efficiency.** Centralizing services that can be shared by multiple workloads, such as network virtual appliances (NVAs) and DNS servers, in a single location allows IT to minimize redundant resources and management effort.
- **Overcoming subscription limits.** Large cloud-based workloads might require using more resources than are allowed in a single Azure subscription. Peering workload virtual networks from different subscriptions to a central hub can overcome these limits. For more information, see [Azure subscription limits](#).
- **Separation of concerns.** You can deploy individual workloads between Central IT teams and workload teams.

Smaller cloud estates might not benefit from the added structure and capabilities that this model offers. But larger cloud adoption efforts should consider implementing a hub and spoke networking architecture if they have any of the concerns listed previously.

## NOTE

The Azure reference architectures site contains example templates that you can use as the basis for implementing your own hub and spoke networks:

- [Implement a hub and spoke network topology in Azure](#)
- [Implement a hub and spoke network topology with shared services in Azure](#)

## Overview

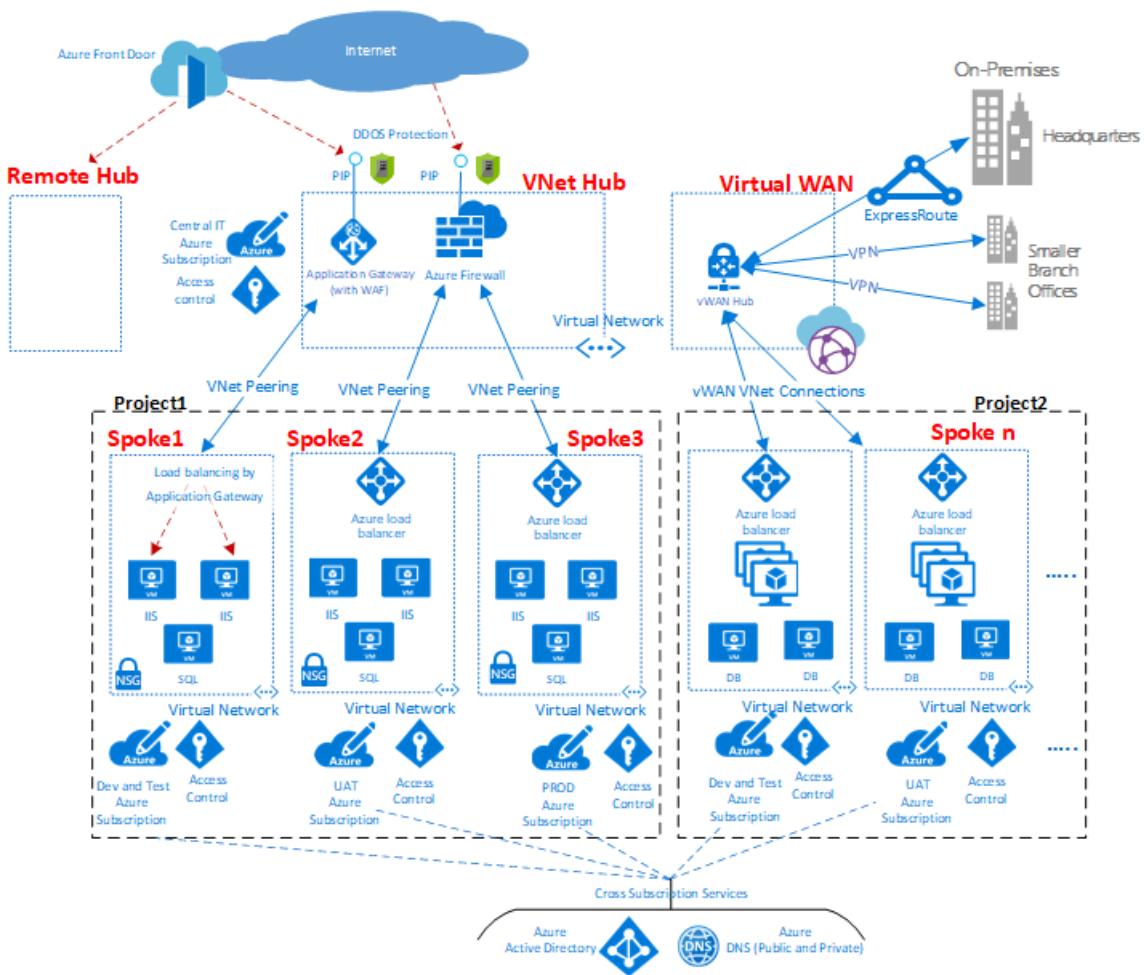


Figure 1: Example of a hub and spoke network topology.

As shown in the diagram, Azure supports two types of hub and spoke design. It supports communication, shared resources, and centralized security policy (labeled as **VNet hub** in the diagram), or a design based on Azure Virtual WAN (labeled as **Virtual WAN** in the diagram) for large-scale branch-to-branch and branch-to-Azure communications.

A hub is a central network zone that controls and inspects ingress or egress traffic between zones: internet, on-premises, and spokes. The hub and spoke topology gives your IT department an effective way to enforce security policies in a central location. It also reduces the potential for misconfiguration and exposure.

The hub often contains the common service components that the spokes consume. The following examples are common central services:

- The Windows server Active Directory infrastructure, required for user authentication of third parties that gain access from untrusted networks before they get access to the workloads in the spoke. It includes the related Active Directory Federation Services (AD FS).
- A DNS service to resolve naming for the workload in the spokes, to access resources on-premises and on the internet if [Azure DNS](#) isn't used.
- A public key infrastructure (PKI), to implement single sign-on on workloads.
- Flow control of TCP and UDP traffic between the spoke network zones and the internet.
- Flow control between the spokes and on-premises.
- If needed, flow control between one spoke and another.

You can minimize redundancy, simplify management, and reduce overall cost by using the shared hub infrastructure to support multiple spokes.

The role of each spoke can be to host different types of workloads. The spokes also provide a modular approach for repeatable deployments of the same workloads. Examples include dev/test, user acceptance testing, staging,

and production.

The spokes can also segregate and enable different groups within your organization. An example is Azure DevOps groups. Inside a spoke, it's possible to deploy a basic workload or complex multitier workloads with traffic control between the tiers.

## Subscription limits and multiple hubs

In Azure, every component, whatever the type, is deployed in an Azure subscription. The isolation of Azure components in different Azure subscriptions can satisfy the requirements of different lines of business, such as setting up differentiated levels of access and authorization.

A single hub and spoke implementation can scale up to a large number of spokes. But as with every IT system, there are platform limits. The hub deployment is bound to a specific Azure subscription, which has restrictions and limits. One example is a maximum number of virtual network peerings. For more information, see [Azure subscription and service limits](#).

In cases where limits might be an issue, you can scale up the architecture further by extending the model from a single hub and spoke to a cluster of hubs and spokes. You can interconnect multiple hubs in one or more Azure regions by using virtual network peering, Azure ExpressRoute, Azure Virtual WAN, or a site-to-site VPN.

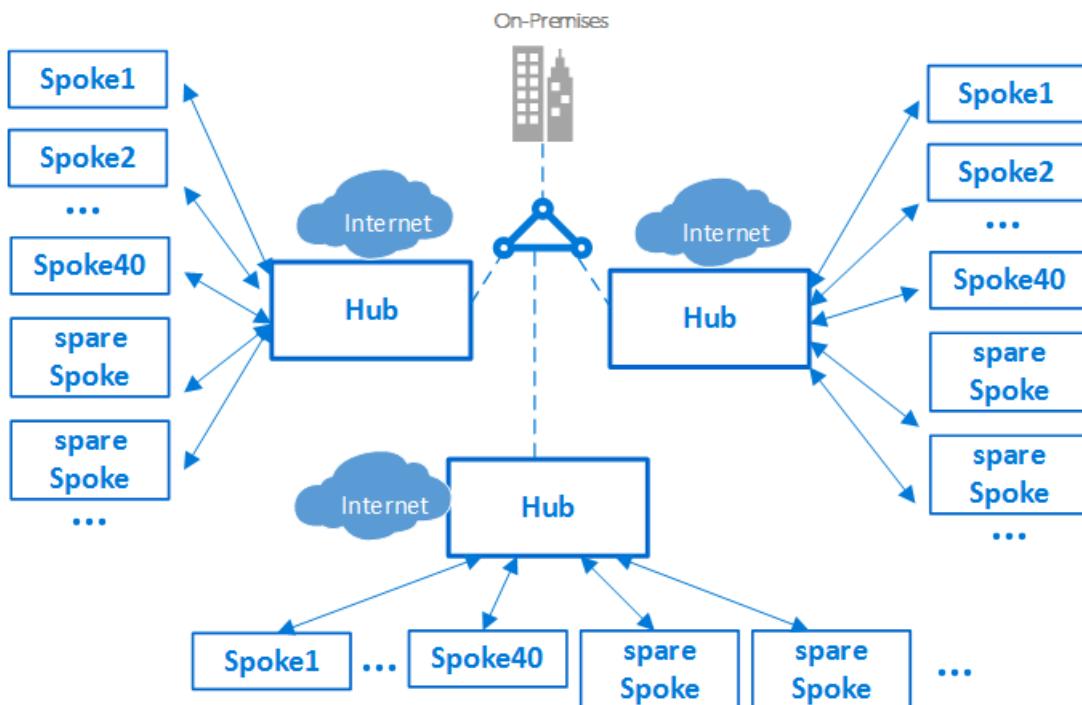


Figure 2: A cluster of hubs and spokes.

The introduction of multiple hubs increases the cost and management overhead of the system. This is only justified by scalability, system limits, or redundancy and regional replication for user performance or disaster recovery. In scenarios that require multiple hubs, all the hubs should strive to offer the same set of services for operational ease.

## Interconnection between spokes

It's possible to implement complex multitier workloads in a single spoke. You can implement multitier configurations by using subnets (one for every tier) in the same virtual network and by using network security groups to filter the flows.

An architect might want to deploy a multitier workload across multiple virtual networks. With virtual network peering, spokes can connect to other spokes in the same hub or in different hubs.

A typical example of this scenario is the case where application processing servers are in one spoke or virtual network. The database deploys in a different spoke or virtual network. In this case, it's easy to interconnect the spokes with virtual network peering and avoid transiting through the hub. The solution is to perform a careful architecture and security review to ensure that bypassing the hub doesn't bypass important security or auditing points that might exist only in the hub.

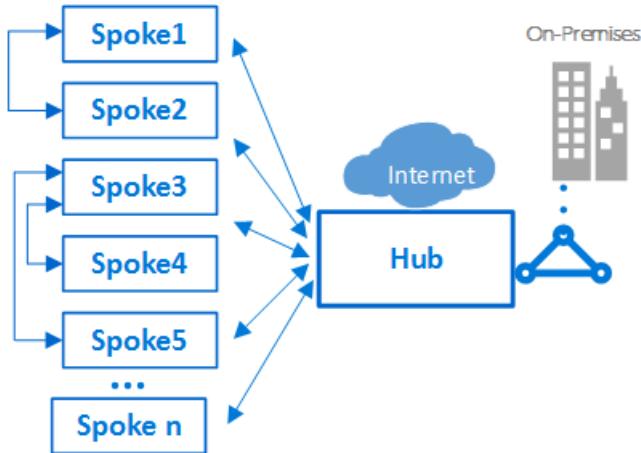


Figure 3: Spokes connecting to each other and a hub.

Spokes can also be interconnected to a spoke that acts as a hub. This approach creates a two-level hierarchy: the spoke in the higher level (level 0) becomes the hub of lower spokes (level 1) of the hierarchy. The spoke implementation is required to forward the traffic to the central hub so that the traffic can transit to its destination in either the on-premises network or the public internet. An architecture with two levels of hubs introduces complex routing that removes the benefits of a simple hub and spoke relationship.

# Track costs across business units, environments, or projects

11/9/2020 • 8 minutes to read • [Edit Online](#)

Building a [cost-conscious organization](#) requires visibility and properly defined access (or scope) to cost-related data. This best-practice article outlines decisions and implementation approaches to creating tracking mechanisms.



Figure 1: Outline of a cost-conscious process.

## Establish a well-managed environment hierarchy

Cost control, much like governance and other management constructs, depends on a well-managed environment. Establishing such an environment (especially a complex one) requires consistent processes in the classification and organization of all assets.

Assets (also known as resources) include all virtual machines, data sources, and applications deployed to the cloud. Azure provides several mechanisms for classifying and organizing assets. [Organize and manage your Azure subscriptions](#) details options for organizing resources based on multiple criteria to establish a well-managed environment. This article focuses on the application of Azure fundamental concepts to provide cloud cost visibility.

### Classification

[Tagging](#) is an easy way to classify assets. Tagging associates metadata to an asset. That metadata can be used to classify the asset based on various data points. When tags are used to classify assets as part of a cost management effort, companies often need the following tags: business unit, department, billing code, geography, environment, project, and workload or "application categorization." Azure Cost Management and Billing can use these tags to create different views of cost data.

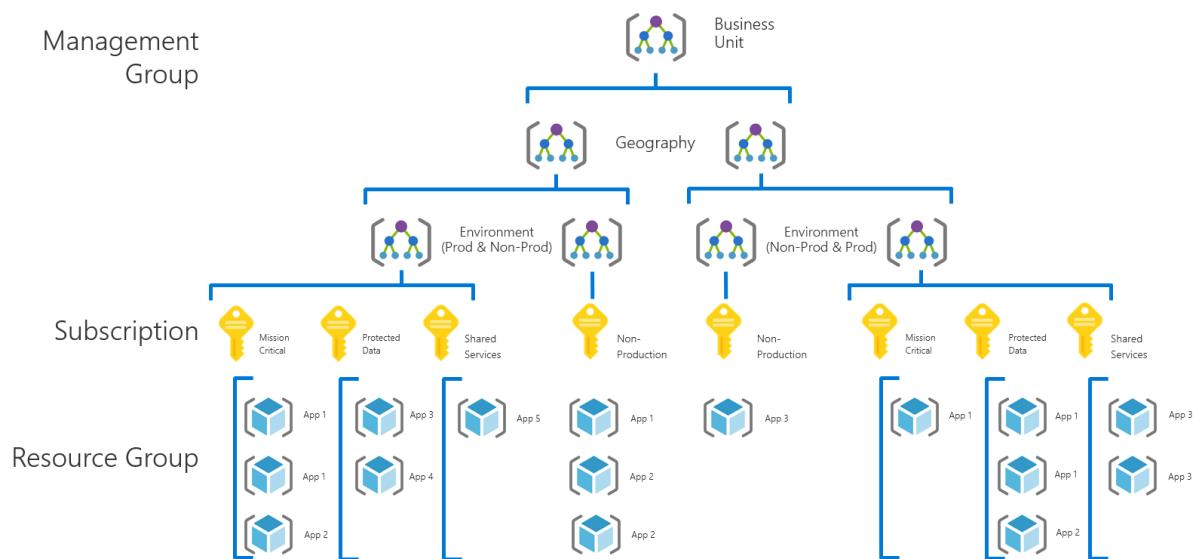
Tagging is a primary way to understand the data in any cost reporting. It's a fundamental part of any well-managed environment. It's also the first step in establishing proper governance of any environment.

The first step in accurately tracking cost information across business units, environments, and projects is to define a tagging standard. The second step is to ensure that the tagging standard is consistently applied. The following articles can help you accomplish: [developing naming and tagging standards](#) and [establishing a governance MVP to enforce tagging standards](#)

## Resource organization

There are several approaches to organizing assets. This section outlines a best practice based on the needs of a large enterprise with cost structures spread across business units, geographies, and IT organizations. A similar best practice for a smaller, less complex organization is available in the [standard enterprise governance guide](#).

For a large enterprise, the following model for management groups, subscriptions, and resource groups will create a hierarchy that allows each team to have the right level of visibility to perform their duties. When the enterprise needs cost controls to prevent budget overrun, it can apply governance tooling like Azure Blueprints or Azure Policy to the subscriptions within this structure to quickly block future cost errors.



*Figure 2: Resource organization for a large enterprise.*

In the preceding diagram, the root of the management group hierarchy contains a node for each business unit. In this example, the multinational company needs visibility into the regional business units, so it creates a node for geography under each business unit in the hierarchy.

Within each geography, there's a separate node for production and nonproduction environments to isolate cost, access, and governance controls. To allow for more efficient operations and wiser operations investments, the company uses subscriptions to further isolate production environments with varying degrees of operational performance commitments. Finally, the company uses resource groups to capture deployable units of a function, called applications.

The diagram shows best practices but doesn't include these options:

- Many companies limit operations to a single geopolitical region. That approach reduces the need to diversify governance disciplines or cost data based on local data-sovereignty requirements. In those cases, a geography node is unnecessary.
- Some companies prefer to further segregate development, testing, and quality control environments into separate subscriptions.
- When a company integrates a cloud center of excellence (CCoE) team, shared services subscriptions in each geography node can reduce duplicated assets.
- Smaller adoption efforts might have a much smaller management hierarchy. It's common to see a single root node for corporate IT, with a single level of subordinate nodes in the hierarchy for various environments. This

isn't a violation of best practices for a well-managed environment. But it does make it more difficult to provide a least-rights access model for cost control and other important functions.

The rest of this article assumes the use of the best-practice approach in the preceding diagram. But the following articles can help you apply the approach to a resource organization that best fits your company:

- [Scale your Azure environment with multiple subscriptions](#)
- [Organize and manage your Azure subscriptions](#)
- [Deploy a governance MVP to govern well-managed environment standards](#)

## Provide the right level of cost access

Managing cost is a team activity. The organization readiness section of the Cloud Adoption Framework defines a small number of core teams and outlines how those teams support cloud adoption efforts. This article expands on the team definitions to define the scope and roles to assign to members of each team for the proper level of visibility into cost management data.

**Roles** define what a user can do to various assets. The **Scope** defines which assets (user, group, service principal, or managed identity) a user can do those things to.

As a general best practice, we suggest a least-privilege model in assigning people to various roles and scopes.

### Roles

Azure Cost Management and Billing supports the following built-in roles for each scope:

- [Owner](#): Can view costs and manage everything, including cost configuration.
- [Contributor](#): Can view costs and manage everything, including cost configuration, but excluding access control.
- [Reader](#): Can view everything, including cost data and configuration, but can't make changes.
- [Cost Management Contributor](#): Can view costs and manage cost configuration.
- [Cost Management Reader](#): Can view cost data and configuration.

As a general best practice, members of all teams should be assigned the role of Cost Management Contributor. This role grants access to create and manage budgets and exports to more effectively monitor and report on costs. But members of the [cloud strategy team](#) should be set to Cost Management Reader only. That's because they're not involved in setting budgets within the Azure Cost Management and Billing tool.

### Scope

The following scope and role settings will create the required visibility into cost management. This best practice might require minor changes to align to asset organization decisions.

- [Cloud adoption team](#). Responsibilities for ongoing optimization changes require Cost Management Contributor access at the resource group level.
  - **Working environment**. At a minimum, the cloud adoption team should already have [Contributor](#) access to all affected resource groups, or at least those groups related to dev/test or ongoing deployment activities. No additional scope setting is required.
  - **Production environments**. When proper separation of responsibility has been established, the cloud adoption team probably won't continue to have access to the resource groups related to its projects. The resource groups that support the production instances of their workloads will need additional scope to give this team visibility into the production cost impact of its decisions. Setting the [Cost Management Contributor](#) scope for production resource groups for this team will allow the team to monitor costs and set budgets based on usage and ongoing investment in the supported workloads.
- [Cloud strategy team](#). Responsibilities for tracking costs across multiple projects and business units require Cost Management Reader access at the root level of the management group hierarchy.

- Assign [Cost Management Reader](#) access to this team at the management group. This will ensure ongoing visibility into all deployments associated with the subscriptions governed by that management group hierarchy.
- **Cloud governance team.** Responsibilities for managing cost, budget alignment, and reporting across all adoption efforts requires Cost Management Contributor access at the root level of the management group hierarchy.
  - In a well-managed environment, the cloud governance team likely has a higher degree of access already, making additional scope assignment for [Cost Management Contributor](#) unnecessary.
- **Cloud center of excellence.** Responsibility for managing costs related to shared services requires Cost Management Contributor access at the subscription level. Additionally, this team might require Cost Management Contributor access to resource groups or subscriptions that contain assets deployed by CCoE automations to understand how those automations affect costs.
  - **Shared services.** When a cloud center of excellence is engaged, best practice suggests that assets managed by the CCoE are supported from a centralized shared service subscription within a hub and spoke model. In this scenario, the CCoE likely has contributor or owner access to that subscription, making additional scope assignment for [Cost Management Contributor](#) unnecessary.
  - **CCoE automation/controls.** The CCoE commonly provides controls and automated deployment scripts to cloud adoption teams. The CCoE has a responsibility to understand how these accelerators affect costs. To gain that visibility, the team needs [Cost Management Contributor](#) access to any resource groups or subscriptions running those accelerators.
- **Cloud operations team.** Responsibility for managing ongoing costs of production environments requires Cost Management Contributor access to all production subscriptions.
  - The general recommendation puts production and nonproduction assets in separate subscriptions that are governed by nodes of the management group hierarchy associated with production environments. In a well-managed environment, members of the operations team likely have owner or contributor access to production subscriptions already, making the [Cost Management Contributor](#) role unnecessary.

## Additional cost management resources

Azure Cost Management and Billing is a well-documented tool for setting budgets and gaining visibility into cloud costs for Azure or AWS. After you establish access to a well-managed environment hierarchy, the following articles can help you use that tool to monitor and control costs.

### **Get started with Azure Cost Management and Billing**

To begin using Azure Cost Management and Billing, see [How to optimize your cloud investment with Azure Cost Management and Billing](#).

### **Use Azure Cost Management and Billing**

- [Create and manage budgets](#)
- [Export cost data](#)
- [Optimize costs based on recommendations](#)
- [Use cost alerts to monitor usage and spending](#)

### **Use Azure Cost Management and Billing to govern AWS costs**

- [Set up AWS Cost and Usage report integration](#)
- [Manage AWS costs](#)

### **Establish access, roles, and scope**

- [Understanding cost management scope](#)

- Setting scope for a resource group

# Skills readiness path during the Ready phase of a migration journey

11/9/2020 • 4 minutes to read • [Edit Online](#)

During the Ready phase of a migration journey, the objective is to prepare for the journey ahead. This phase is accomplished in two primary areas: organizational readiness and environmental (technical) readiness. Each area might require new skills for both technical and nontechnical contributors. The following sections describe a few options to help build the necessary skills.

## Organizational readiness learning paths

Depending on the motivations and business outcomes associated with a cloud adoption effort, leaders might be required to establish new organizational structures or virtual teams to facilitate various functions. The following articles help to develop the skills that are necessary to structure those teams in accordance with desired outcomes:

- [Initial organization alignment](#): Overview of organizational alignment and various team structures to facilitate specific goals.
- [Break down silos and fiefdoms](#): Understand two common organizational anti-patterns and ways to guide the team to productive collaboration.

## Environmental (technical) readiness learning paths

During the Ready phase, technical staff are called upon to create a migration landing zone that's capable of hosting, operating, and governing workloads that were migrated to the cloud. Developing the necessary skills can be accelerated with the following learning paths:

- [Create an Azure account](#): The first step to using Azure is to create an account. Your account holds the Azure services you provision and handles your personal settings like identity, billing, and preferences.
- [Azure portal](#): Tour the Azure portal features and services, and customize the portal.
- [Introduction to Azure](#): Get started with Azure by creating and configuring your first virtual machine in the cloud.
- [Introduction to security in Azure](#): Discuss the basic concepts for protecting your infrastructure and data when you work in the cloud. Understand what responsibilities are yours and what Azure takes care of for you.
- [Manage resources in Azure](#): Learn how to work with the Azure command line and web portal to create, manage, and control cloud-based resources.
- [Create a VM](#): Create a virtual machine by using the Azure portal.
- [Azure networking](#): Learn some of the Azure networking basics and how Azure networking helps improve resiliency and reduce latency.
- [Azure compute options](#): Review the Azure compute services.
- [Secure resources with role-based access control \(RBAC\)](#): Use RBAC to secure resources.
- [Data storage options](#): Benefits of Azure data storage.

During the Ready phase, architects are called upon to architect solutions that span all Azure environments. The following skill-building resources can prepare architects for these tasks:

- [Foundations for cloud architecture](#): A Pluralsight course to help architect the right foundational solutions.
- [Microsoft Azure architecture](#): A Pluralsight course to ground architects in Azure architecture.
- [Designing migrations for Microsoft Azure](#): A Pluralsight course to help architects design a migration solution.

# Deeper skills exploration

Beyond these initial options for developing skills, there are a variety of learning options available.

## Typical mappings of cloud IT roles

Microsoft and partners offer a variety of options for all audiences to develop their skills with Azure services:

- **Microsoft IT Pro Career Center:** Serves as a free online resource to help map your cloud career path. Learn what industry experts suggest for your cloud role and the skills to get you there. Follow a learning curriculum at your own pace to build the skills you need most to stay relevant.

Turn your knowledge of Azure into official recognition with [Microsoft Azure certification training and exams](#).

## Microsoft Learn

Microsoft Learn is a new approach to learning. Readiness for the new skills and responsibilities that come with cloud adoption doesn't come easily. Microsoft Learn provides a more rewarding approach to hands-on learning that helps you achieve your goals faster. Earn points and levels and achieve more.

The following examples are a few tailored learning paths on Microsoft Learn, which align to the Ready methodology of the Cloud Adoption Framework:

[Azure fundamentals:](#) Learn cloud concepts such as high availability, scalability, elasticity, agility, fault tolerance, and disaster recovery. Understand the benefits of cloud computing in Azure and how it can save you time and money. Compare and contrast basic strategies for transitioning to the Azure cloud. Explore the breadth of services available in Azure including compute, network, storage, and security.

[Manage resources in Azure:](#) Learn how to work with the Azure command line and web portal to create, manage, and control cloud-based resources.

[Administer infrastructure resources in Azure:](#) Learn how to create, manage, secure, and scale virtual machine resources.

[Store data in Azure:](#) Azure provides a variety of ways to store data: unstructured, archival, relational, and more. Learn the basics of storage management in Azure, how to create a storage account, and how to choose the right model for the data you want to store in the cloud.

[Architect great solutions in Azure:](#) Learn how to design and build secure, scalable, and high-performing solutions in Azure by examining the core principles found in sound architecture.

## Learn more

For additional learning paths, browse the [Microsoft Learn catalog](#). Use the **Roles** filter to align learning paths with your role.

# Cloud migration in the Cloud Adoption Framework

11/9/2020 • 4 minutes to read • [Edit Online](#)

Any enterprise-scale [cloud adoption plan](#), will include workloads that do not warrant significant investments in the creation of new business logic. Those workloads could be moved to the cloud through any number of approaches: lift and shift; lift and optimize; or modernize. Each of these approaches is considered a migration. The following exercises will help establish the iterative processes to assess, migrate, optimize, secure, and manage those workloads.

To prepare you for this phase of the cloud adoption lifecycle, we recommend the following:

	<p><a href="#">Migrate your first workload</a>: Use the Azure migration guide to become familiar with the Azure native tools and approach to migration.</p>
	<p><a href="#">Migration scenarios</a>: Use additional migration tools and approaches to act on other migration scenarios.</p>
	<p><a href="#">Best practices</a>: Address common migration needs through the application of consistent best practices.</p>
	<p><a href="#">Process improvements</a>: Migration is a process heavy activity. As migration efforts scale, use these process improvements to evaluate and mature various aspects of migration.</p>

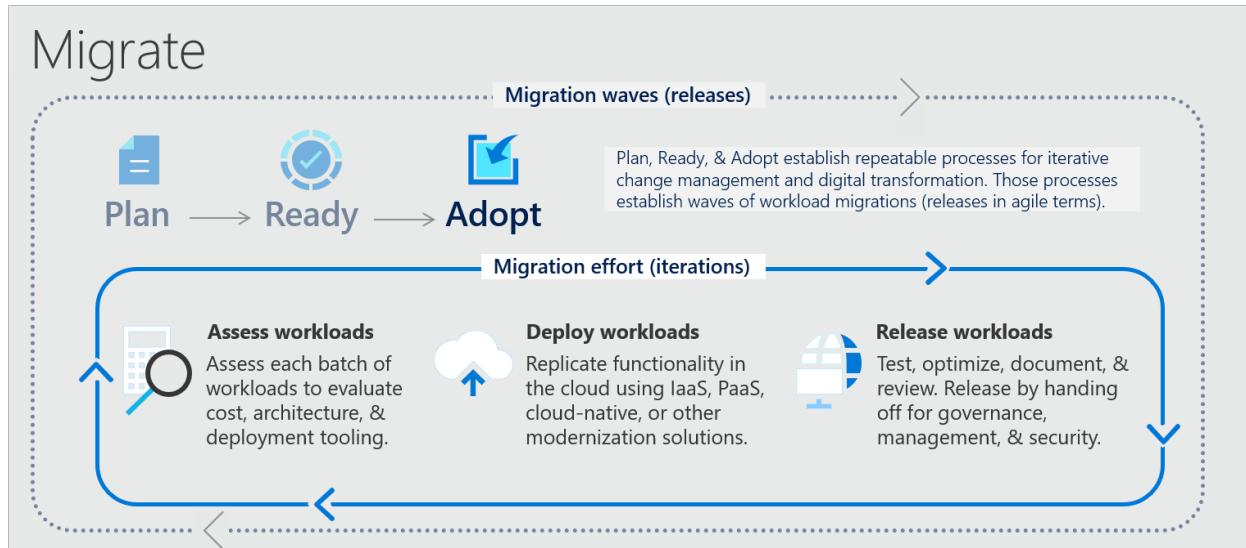
The Migrate methodology and the steps above build on the following assumptions:

- The methodology governing migration sprints fits within migration waves or releases, which are defined using the Plan, Ready, and Adopt methodologies. Within each migration sprint, a batch of workloads is migrated to the cloud.
- Before migrating workloads, at least one [landing zone](#) has been identified, configured, and deployed to meet the needs of the near-term cloud adoption plan.
- Migration is commonly associated with the terms *lift and shift* or *rehost*. This methodology and the above steps are built on the belief that no datacenter and few workloads should be migrated using a pure rehost approach. While many workloads can be rehosted, customers more often choose to modernize specific assets within each workload. During this iterative process, the balance between speed and modernization is a common discussion point.

## Migration effort

The effort required to migrate workloads generally falls into three types of effort (or phases) for each workload: assess workloads, deploy workloads, and release workloads. This section of the Cloud Adoption Framework teaches readers how to maximize the return from each phase required to migrate a workload to production.

In a standard two-week long iteration, an experienced migration team can complete this process for 2-5 workloads of low-medium complexity. More complex workloads, such as SAP, may take several two-week iterations to complete all three phases of migration effort for a single workload. Experience and complexity both have a significant impact on timelines and migration velocity.



The following bullets provide an overview of the phases of this process (pictured above):

- **Assess workloads:** Assess workloads to evaluate cost, modernization, and deployment tooling. This process focuses on validating or challenging the assumptions made during earlier discovery and assessments by looking more closely at rationalization options. This is also when user patterns and dependencies are studied more closely to ensure workloads will achieve technical success after migration.
- **Deploy workloads:** After workloads are assessed, the existing functionality of those workloads is replicated (or improved) in the cloud. This could involve a *lift and shift* or *rehost* to the cloud. But more commonly during this phase, many of the assets supporting these workloads will be modernized to capitalize on the benefits of the cloud.
- **Release workloads:** Once functionality is replicated to the cloud, workloads can be tested, optimized, documented, and released for ongoing operations. Critical during this process, is the effort to review the migrated workloads and hand them off to governance, operations management, and security teams for ongoing support of those workloads.

#### NOTE

In some early iterations of migration effort, it is common to limit scope to a single workload. This approach maximizes skills retention and provides the team with more time to experiment and learn.

#### NOTE

When building a migration factory, some teams may choose to disperse each of the above phases across multiple teams and multiple sprints. This approach can improve repeatability and accelerate migration efforts.

## Migration waves and iterative change management

Migration iterations deliver technical value by migrating assets and workloads. A migration wave is the smallest collection of workloads that deliver tangible and measurable business value. Each iteration should result in a

report outlining the technical efforts completed. However, business change and strategic planning typically happen at a slightly higher level. As the cloud adoption team delivers on the migration effort, the cloud strategy team focuses on planning the next 1-2 migration waves. The cloud strategy team also tracks technical progress as a learning metric to better understand the timelines for realizing business value. In that regard, migration waves are the iterative change management approach to tracking business outcomes, people, and timelines.

As outlined in the graphic in the prior section, processes within the [Plan methodology](#), the [Ready methodology](#), and to some extent the [Strategy methodology](#) of the Cloud Adoption Framework provide guidance on planning and managing the migration waves. The management of those waves will prioritize and define the migration effort to be delivered by the technical teams.

## Next steps

The steps outlined above, and subsequent guidance in the Migrate methodology, can help you develop skills to improve processes within each migration sprint. The [Azure migration guide](#) is a brief series of articles that outlines the most common tools and approaches needed during your first migration wave.

[Azure migration guide](#)

# Azure migration guide overview

11/9/2020 • 2 minutes to read • [Edit Online](#)

The [Cloud Adoption Framework's Migrate methodology](#) guides readers through an iterative process of migrating one workload, or a small collection of workloads per release. In each iteration, the process of assess, migration, and optimize and promote is followed to ensure that workloads are ready to meet production demands. That cloud-agnostic process can guide migration to any cloud provider.

This guide demonstrates a simplified version of that process when migrating from your on-premises environment to **Azure**.

## TIP

For an interactive experience, view this guide in the Azure portal. Go to the [Azure Quickstart Center](#) in the Azure portal, select **Azure migration guide**, and then follow the step-by-step instructions.

- [Migration tools](#)
- [When to use this guide](#)

This guide is the suggested path for your first migration to Azure, as it will expose you to the methodology and the cloud-native tools most commonly used during migration to Azure. Those tools are presented across the following pages:

- **Assess each workload's technical fit.** Validate the technical readiness and suitability for migration.
- **Migrate your services.** Perform the actual migration, by replicating on-premises resources to Azure.
- **Manage costs and billing.** Understand the tools required to control costs in Azure.
- **Optimize and promote.** Optimize for cost and performance balance before promoting your workload to production.
- **Get assistance.** Get help and support during your migration or post-migration activities.

It is assumed that a landing zone has already been deployed, in alignment with the best practices in the [Cloud Adoption Framework's Ready methodology](#).

# Assess workloads and refine plans

11/9/2020 • 7 minutes to read • [Edit Online](#)

The resources in this guide help you assess each workload, challenge assumptions about each workload's suitability for migration, and finalize architectural decisions about migration options.

- [Tools](#)
- [Challenge assumptions](#)
- [Scenarios and stakeholders](#)
- [Timelines](#)
- [Cost management](#)

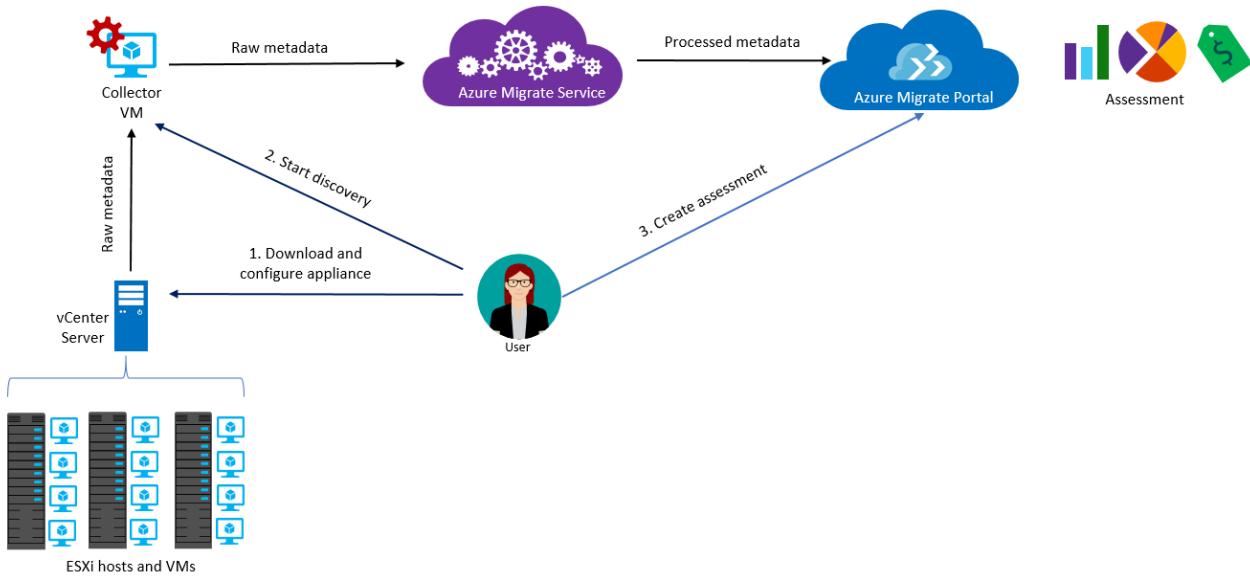
If you didn't follow the guidance in the links above, you will likely need data and an assessment tool to make informed migration decisions. Azure Migrate is the native tool for assessing **and** migrating to Azure. If you haven't already, use these steps to create a new server migration project and collect the necessary data.

## Azure Migrate

Azure Migrate assesses on-premises infrastructure, applications, and data for migration to Azure. This service:

- Assesses the migration suitability of on-premises assets.
- Performs performance-based sizing.
- Provides cost estimates for running on-premises assets in Azure.

If you're considering a lift and shift approach, or are in the early assessment stages of migration, this service is for you. After completing the assessment, use Azure Migrate to execute the migration.



### Create a new server migration project

Begin a server migration assessment using Azure Migrate via these steps:

1. Select **Azure Migrate**.
2. In **Overview**, select **Assess and migrate servers**.
3. Select **Add tools**.
4. In **Discover, assess and migrate servers**, select **Add tools**.
5. In **Migrate project**, select your Azure subscription, then create a resource group if you don't have one.

6. In **Project Details**, specify the project name and geography where you want to create the project, then select **Next**.
7. In **Select assessment tool**, select **Skip adding an assessment tool for now > Next**.
8. In **Select migration tool**, select **Azure Migrate: Server Migration > Next**.
9. In **Review + add tools**, review the settings, then select **Add tools**.
10. After adding the tool, it appears in **Azure Migrate project > Servers > Migration tools**.



#### Learn more

- [Azure Migrate overview](#)
- [Migrate physical or virtualized servers to Azure](#)
- [Azure Migrate in the Azure portal](#)

#### Service Map

Service Map automatically discovers application components on Windows and Linux systems and maps the communication between services. With Service Map, you can view your servers in the way that you think of them: as interconnected systems that deliver critical services. Service Map shows connections between servers, processes, inbound and outbound connection latency, and ports across any TCP-connected architecture, with no configuration required other than the installation of an agent.

Azure Migrate uses Service Map to enhance the reporting capabilities and dependencies across the environment. For full details of this integration, see [Dependency visualization](#). If you use the Azure Migrate service, then no additional steps are required to configure and obtain the benefits of Service Map. The following instructions are provided for your reference if you'd like to use Service Map for other purposes or projects.

#### Enable dependency visualization using Service Map

To use dependency visualization, download and install agents on each on-premises machine that you want to analyze.

- [Microsoft Monitoring Agent](#) must be installed on each machine.
- The [Microsoft Dependency Agent](#) must be installed on each machine.
- Also, if you have machines with no internet connectivity, download and install Log Analytics gateway on those machines.

#### Learn more

- [Using Service Map solution in Azure](#)
- [Azure Migrate and Service Map: Dependency visualization](#)

# Deploy workloads and assets (infrastructure, apps, and data)

11/9/2020 • 11 minutes to read • [Edit Online](#)

In this phase of the journey, you use the output of the Assess phase to initiate the migration of the environment. This guide helps identify the appropriate tools to reach a completed state. You'll explore native tools, third-party tools, and project management tools.

- [Native migration tools](#)
- [Third-party migration tools](#)
- [Project management tools](#)
- [Cost management](#)

The following sections describe the native Azure tools available to perform or assist with migration. For information on choosing the right tools to support your migration efforts, see the [Cloud Adoption Framework's migration tools decision guide](#).

## Azure Migrate

Azure Migrate delivers a unified and extensible migration experience. Azure Migrate provides a one-stop, dedicated experience to track your migration journey across the phases of assessment and migration to Azure. It provides you the option to use the tools of your choice and track the progress of migration across these tools.

Azure Migrate is a centralized hub to assess and migrate on-premises servers, infrastructure, applications, and data to Azure. It provides the following functionality:

- Unified platform with assessment, migration, and progress tracking.
- Enhanced assessment and migration capabilities:
  - On-premises servers including Hyper-V & VMware.
  - Agentless migration of VMware virtual machines to Azure.
  - Database migrations to Azure SQL Database or SQL Managed Instance
  - Web applications
  - Virtual desktop infrastructure (VDI) to Windows Virtual Desktop in Azure
  - Large data collections using Azure Data Box products
- Extensible approach with ISV integration (such as Cloudamize).

To perform a migration using Azure Migrate, follow these steps:

1. Search for Azure Migrate under **All services**. Select **Azure Migrate** to continue.
2. Select **Add a tool** to start your migration project.
3. Select the subscription, resource group, and geography to host the migration.
4. Select **Select assessment tool > Azure Migrate: Server assessment > Next**.
5. Select **Review + add tools**, and verify the configuration. Select **Add tools** to initiate the job to create the migration project and register the selected solutions.

### NOTE

For guidance specific to your scenario refer to the tutorials and Azure Migrate [documentation](#).

[Learn more](#)

- [About Azure Migrate](#)
- [Azure Migrate tutorial - migrate physical or virtualized servers to Azure](#)

## Azure Database Migration Service

Azure Database Migration Service is a fully managed service that enables seamless migrations from multiple database sources to Azure data platforms, with minimal downtime (online migrations). Database Migration Service performs all of the required steps. You can initiate your migration projects assured that the process takes advantage of best practices recommended by Microsoft.

### Create an Azure Database Migration Service instance

If this is the first time using Azure Database Migration Service, you need to register the resource provider for your Azure subscription:

1. Select **All services > Subscriptions**, and choose the target subscription.
2. Select **Resource providers**.
3. Search for **migration**, and then to the right of **Microsoft.DataMigration**, select **Register**.



After you register the resource provider, you can create an instance of Azure Database Migration Service.

1. Select **+ Create a resource** and search the marketplace for **Azure Database Migration Service**.
2. Complete the Create Migration Service Wizard, then select **Create**.

The service is now ready to migrate the supported source databases to target platforms such as SQL Server, MySQL, PostgreSQL, or MongoDB.



For more information, see:

- [Azure Database Migration Service overview](#)
- [Create an instance of Azure Database Migration Service](#)
- [Azure Migrate in the Azure portal](#)
- [Azure portal: Create a migration project](#)

## Azure App Service Migration Assistant

The Azure App Service Migration Assistant is part of a [larger suite of applications](#) that help organizations with their transition to the cloud. The Migration Assistant provides a guided, wizard-like user experience that performs two tasks:

1. It performs an assessment of a specific web app installed on Windows Server by running pre-migration compatibility checks on the web app to determine whether a migration to Azure App Service is possible without modification to the web app.
2. If the assessment proves that the web app can be migrated, the Migration Assistant performs the migration. You'll need to give the Migration Assistant access to your Azure account, select which resource group you want to use, and select a name for the web app, among other details. Alternatively, the Migration Assistant generates an Azure Resource Manager template that you can use to migrate the web application in a more automated and repeatable way.

### Migrate a web app to Azure App Service

The Migration Assistant begins the migration process by collecting key details from you about your Azure account and then performs the migration.

First, you'll sign in to your Azure account and associate your Migration Assistant session with your account by

using a unique code. Next, you'll choose the subscription, the resource group, and the website's domain name. You can choose to create a new Azure App Service plan to host the app or select an existing plan. The choice affects the geographical region from which your app is hosted. You'll also have a chance to associate this migration effort with an existing Azure Migrate project. Finally, you can either choose to skip database setup or choose to set up a hybrid connection to enable a database connection.

After the Migration Assistant collects and verifies your selections, it creates the needed Azure App Service resources in the selected region and resource group. It zips up the web app's source files and uses the Azure App Service deployment API to deploy them. Finally, it performs optional migration steps, like helping you set up a hybrid connection.

After a successful migration, you'll need to perform any post-migration tasks. These might include:

- Manually moving application settings and connection strings in your web.config file to Azure App Service.
- Migrating data from an on-premises SQL Server instance to an Azure SQL database.
- Setting up an SSL certificate.
- Setting up custom domain names.
- Setting up permissions in Azure Active Directory.

You might also decide to change the Azure App Service hosting plan and other settings like autoscaling and deployment slots.

For more information see:

## [Migrate ASP.NET Apps to Azure](#)

### **Data Migration Assistant**

Data Migration Assistant (DMA) helps you upgrade to a modern data platform by detecting compatibility issues that can affect database functionality in your new version of SQL Server or Azure SQL Database. DMA recommends performance and reliability improvements for your target environment and allows you to move your schema, data, and uncontained objects from your source server to your target server.

Data Migration Assistant is integrated with Azure Migrate, allowing you to track all assessment progress in the Azure Migrate dashboard. Launch DMA from Azure Migrate by adding the Azure Migrate: Database Assessment tool, and add your database assessment to Azure Migrate by selecting the "Upload to Azure Migrate" button in DMA.

#### **NOTE**

For large migrations (in terms of number and size of databases), we recommend that you use Azure Database Migration Service, which can migrate databases at scale.

Start using Data Migration Assistant with these steps:

1. Download and install Data Migration Assistant from the [Microsoft download center](#).
2. Create an assessment by selecting the **New (+)** icon, then select the **Assessment** project type.
3. Set the source and target server type, then select **Create**.
4. Configure the assessment options as required (recommend all defaults).
5. Add the databases to assess.
6. Select **Next** to start the assessment.
7. View results in Data Migration Assistant.

For an enterprise, we recommend following the approach outlined in [Assess an enterprise and consolidate assessment reports with DMA](#) to assess multiple servers, combine the reports, and then use provided Power BI reports to analyze the results.

For more information, including detailed usage steps, see:

- [Data Migration Assistant overview](#)
- [Assess an enterprise and consolidate assessment reports with DMA](#)
- [Analyze consolidated assessment reports created by Data Migration Assistant with Power BI](#)

### **SQL Server migration assistant**

Microsoft SQL Server migration assistant (SSMA) is a tool designed to automate database migration to SQL Server from Microsoft access, DB2, MySQL, Oracle, and SAP ASE. The general concept is to collect, assess, and then review with these tools, however, due to the variances in the process for each of the source systems we recommend reviewing the detailed [SQL Server migration assistant documentation](#).

For more information, see:

- [SQL Server migration assistant overview](#)

### **Database experimentation assistant**

Database experimentation assistant (DEA) is a new A/B testing solution for SQL Server upgrades. It will assist in evaluating a targeted version of SQL for a given workload. Customers who are upgrading from previous SQL Server versions (SQL Server 2005 and above) to any new version of the SQL Server can use these analysis metrics.

The database experimentation assistant contains the following workflow activities:

- **Capture:** The first step of SQL Server a/B testing is to capture a trace on your source server. The source server usually is the production server.
- **Replay:** The second step of SQL Server a/B testing is to replay the trace file that was captured to your target servers. Then, collect extensive traces from the replays for analysis.
- **Analysis:** The final step is to generate an analysis report by using the replay traces. The analysis report can help you gain insight about the performance implications of the proposed change.

For more information, see:

- [Overview of database experimentation assistant](#)

### **Azure Cosmos DB data migration tool**

Azure Cosmos DB data migration tool can import data from various sources into Azure Cosmos DB collections and tables. You can import from JSON files, CSV files, SQL, MongoDB, Azure Table storage, Amazon DynamoDB, and even Azure Cosmos DB SQL API collections. The data migration tool can also be used when migrating from a single partition collection to a multipartition collection for the SQL API.

For more information, see:

- [Azure Cosmos DB data migration tool](#)

# Release workloads (test, optimize, and handoff)

11/9/2020 • 3 minutes to read • [Edit Online](#)

Now that you have migrated your services to Azure, the next phase includes reviewing the solution for possible areas of optimization. This effort could include reviewing the design of the solution, right-sizing the services, and analyzing costs.

This phase is also an opportunity to optimize your environment and perform possible transformations of the environment. For example, you may have performed a "rehost" migration, and now that your services are running on Azure you can revisit the solutions configuration or consumed services, and possibly perform some "refactoring" to modernize and increase the functionality of your solution.

The remainder of this article focuses on tools for optimizing the migrated workload. When the proper balance between performance and cost has been reached, a workload is ready to be promoted to production. For guidance on promotion options, see the process improvement articles on [optimize and promote](#).

- [Right-size assets](#)
- [Cost management](#)

All Azure services that provide a consumption-based cost model can be resized through the Azure portal, CLI, or PowerShell. The first step in correctly sizing a service is to review its usage metrics. The Azure Monitor service provides access to these metrics. You may need to configure the collection of the metrics for the service you're analyzing, and allow an appropriate time to collect meaningful data based on your workload patterns.

1. Go to [Monitor](#).
2. Select [Metrics](#) and configure the chart to show the metrics for the service to analyze.



The following are some common services that you can resize.

## Resize a virtual machine

Azure Migrate performs a right-sizing analysis as part of its pre-migration Assess phase, and virtual machines migrated using this tool will likely already be sized based on your pre-migration requirements.

However, for virtual machines created or migrated using other methods, or in cases where your post-migration virtual machine requirements need adjustment, you may want to further refine your virtual machine sizing.

1. Go to [Virtual machines](#).
2. Select the desired virtual machine from the list.
3. Select [Size](#) and the desired new size from the list. You may need to adjust the filters to find the size you need.
4. Select [Resize](#).

Resizing production virtual machines can cause service disruptions. Try to apply the correct sizing for your VMs before you promote them to production.



- [Manage reservations for Azure resources](#)
- [Resize a Windows VM](#)
- [Resize a Linux virtual machine using Azure CLI](#)

Partners can use the Partner Center to review the usage.

- [Azure VM sizing for maximum reservation usage](#)

### Resize a storage account

1. Go to [Storage accounts](#).
2. Select the desired storage account.
3. Select **Configure** and adjust the properties of the storage account to match your requirements.
4. Select **Save**.

GO TO STORAGE  
ACCOUNTS

### Resize a SQL Database

1. Go to either [SQL databases](#), or [SQL servers](#), then select the server.
2. Select the desired database.
3. Select **Configure** and the desired new service tier size.
4. Select **Apply**.

GO TO SQL  
DATABASES

# Migration-focused cost control mechanisms

11/9/2020 • 7 minutes to read • [Edit Online](#)

The cloud introduces a few shifts in how we work, regardless of our role on the technology team. Cost is a great example of this shift. In the past, only finance and IT leadership were concerned with the cost of IT assets (infrastructure, apps, and data). The cloud empowers every member of IT to make and act on decisions that better support the end user. However, with that power comes the responsibility to be cost conscious when making those decisions.

This article introduces the tools that can help make wise cost decisions before, during, and after a migration to Azure.

The tools in this article include:

- Azure Migrate
- Azure pricing calculator
- Azure TCO calculator
- Azure Cost Management and Billing
- Azure Advisor

The processes described in this article may also require a partnership with IT managers, finance, or line-of-business application owners.

- [Estimate VM costs prior to migration](#)
- [Estimate and optimize VM costs during and after migration](#)
- [Tips and tricks to optimize costs](#)

Prior to migration of any asset (infrastructure, app, or data), there is an opportunity to estimate costs and refine sizing based on observed performance criteria for those assets. Estimating costs serves two purposes: it allows for cost control, and it provides a checkpoint to ensure that current budgets account for necessary performance requirements.

## Cost calculators

For manual cost calculations, there are two handy calculators that can provide a quick cost estimate based on the architecture of the workload to be migrated.

- The [Azure pricing calculator](#) provides cost estimates for the Azure products you select.
- Sometimes decisions require a comparison of the future cloud costs and the current on-premises costs. The [total cost of ownership \(TCO\) calculator](#) can provide such a comparison.

These manual cost calculators can be used on their own to forecast potential spend and savings. They can also be used in conjunction with the cost forecasting tools of Azure Migrate to adjust the cost expectations to fit alternative architectures or performance constraints.

## Azure Migrate calculations

**Prerequisites:** The remainder of this tab assumes the reader has already populated Azure Migrate with a collection of assets (infrastructure, apps, and data) to be migrated. The prior article on assessments provides instructions on collecting the initial data. Once the data is populated, follow the next few steps to estimate monthly costs based on the data collected.

Azure Migrate calculates monthly cost estimates based on data captured by the collector and Service Map. The

following steps will load the cost estimates:

1. Navigate to **Azure Migrate assessment** in the portal.
2. In the project **Overview** page, select + **Create assessment**.
3. Select **View all** to review the assessment properties.
4. Create the group, and specify a group name.
5. Select the machines that you want to add to the group.
6. Select **Create assessment**, to create the group and the assessment.
7. After the assessment is created, view it in **Overview > Dashboard**.
8. In the **Assessment details** section of the portal navigation, select **Cost details**.

The resulting estimate, pictured below, identifies the monthly costs of compute and storage, which often represent the largest portion of cloud costs.

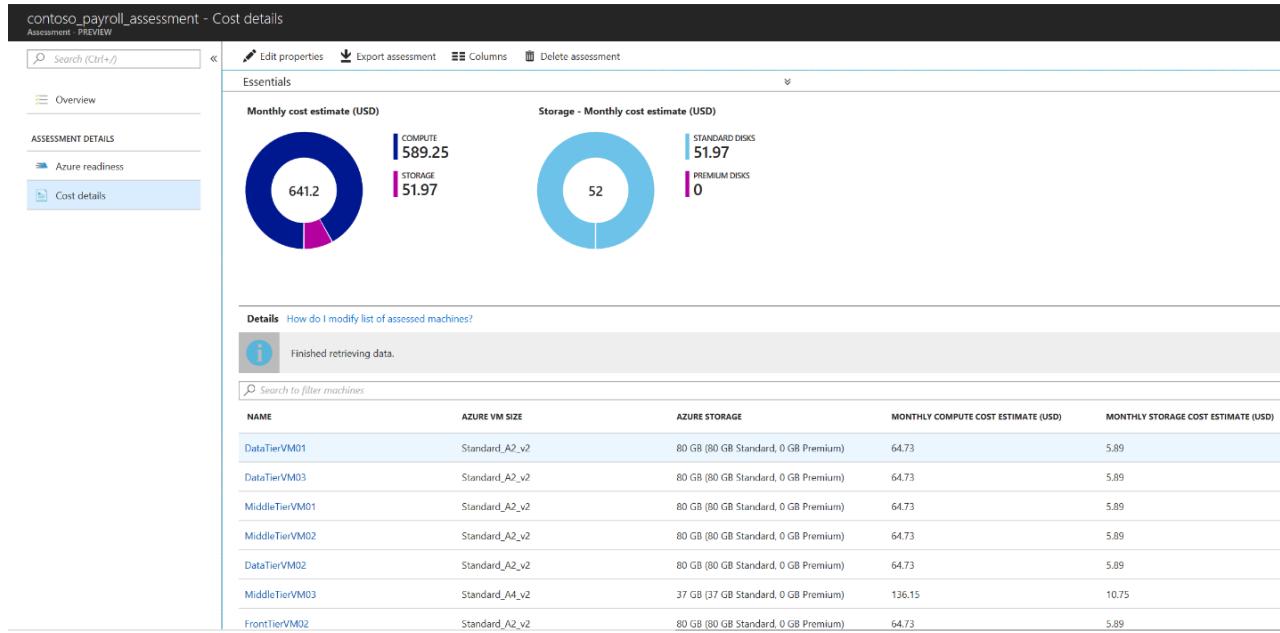


Figure 1: Diagram of the cost details view of an assessment in Azure Migrate.

## Additional resources

- [Set up and review an assessment with Azure Migrate](#)
- For a more comprehensive plan on cost management across larger numbers of assets (infrastructure, apps, and data), see the [Cloud Adoption Framework governance model](#). In particular, see [Cost Management discipline guidance](#) and [Cost Management discipline improvement](#).

# Get assistance

11/9/2020 • 2 minutes to read • [Edit Online](#)

We know that getting the right support at the right time will accelerate your migration efforts. Review the assistance avenues below to meet your needs.

- [Support plans](#)
- [Partners](#)

## Microsoft Support

Microsoft offers a basic support plan to all Azure customers. You have 24x7 access to billing and subscription support, online self-help, documentation, whitepapers, and support forums.

If you need help from Microsoft Support while using Azure, follow these steps to create a support request:

1. Select **Help + support** in the [Azure portal](#).
2. Select **New support request** to enter details about your issue and contact support.
  
1. Select **Help + support**.
2. Select **New support request** to enter details about your issue and contact support.

CREATE A SUPPORT  
REQUEST

To view your support requests, follow these steps:

1. Select **Help + support** in the [Azure portal](#).
2. Select **All support requests** to view your support requests.
  
1. Select **Help + support**.
2. Select **All support requests** to view your support requests.

VIEW YOUR SUPPORT  
REQUESTS

Need support engineer assistance for deep technical guidance?

1. Select **Help + support** in the [Azure portal](#).
2. Select **Support Plans** to review the plans available to you.
  
1. Select **Help + support**.
2. Select **Support Plans** to review the plans available to you.

REVIEW SUPPORT  
PLANS

## Online communities

The following online communities provide community-based support:

- [MSDN forums](#)
- [Stack Overflow](#)

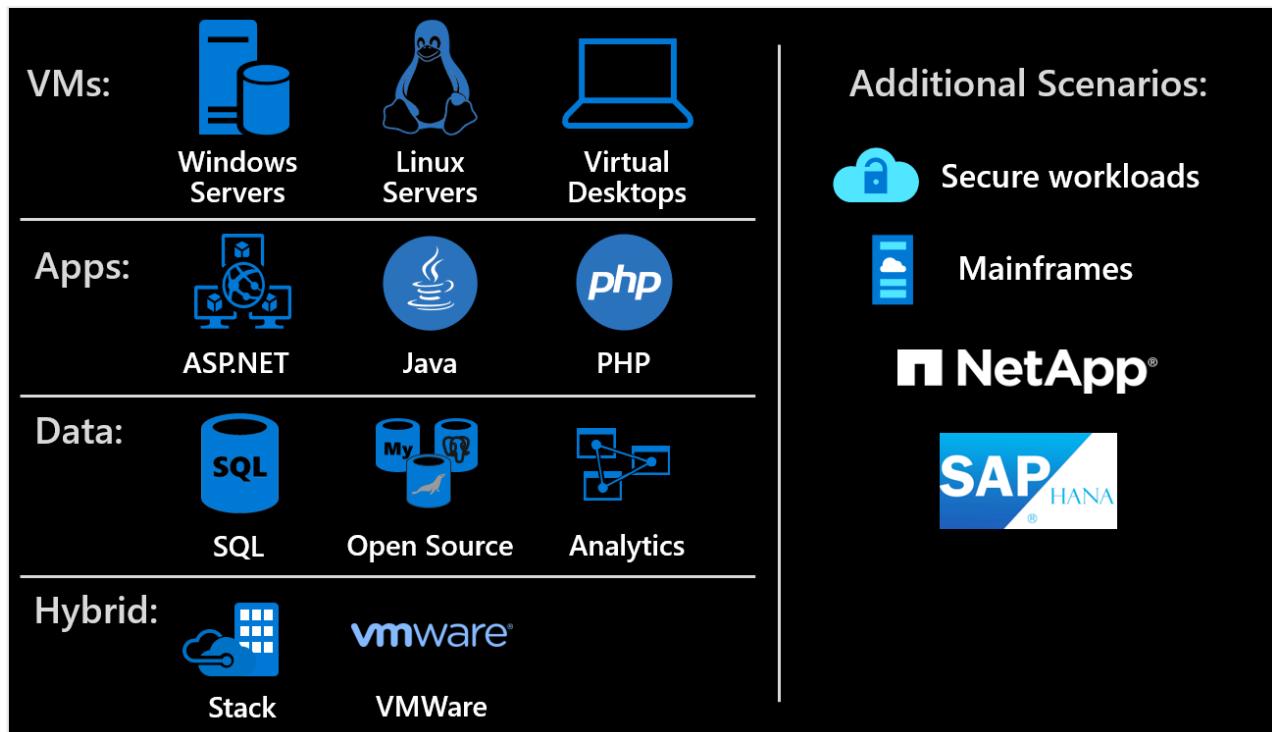
# The One Migration approach to migrating the IT portfolio

11/9/2020 • 2 minutes to read • [Edit Online](#)

Azure and Azure Migrate are both well known for hosting Microsoft technologies. But you might not be aware of Azure's ability to support migrations beyond Windows and SQL Server. The *One Migration* scenarios captured in the Migrate methodology demonstrate the same set of consistent guidelines and processes for migrating both Microsoft and third-party technologies.

## Migration scenarios

The following diagram and table outline a number of scenarios that follow the same iterative Migrate methodology for migration and modernization.

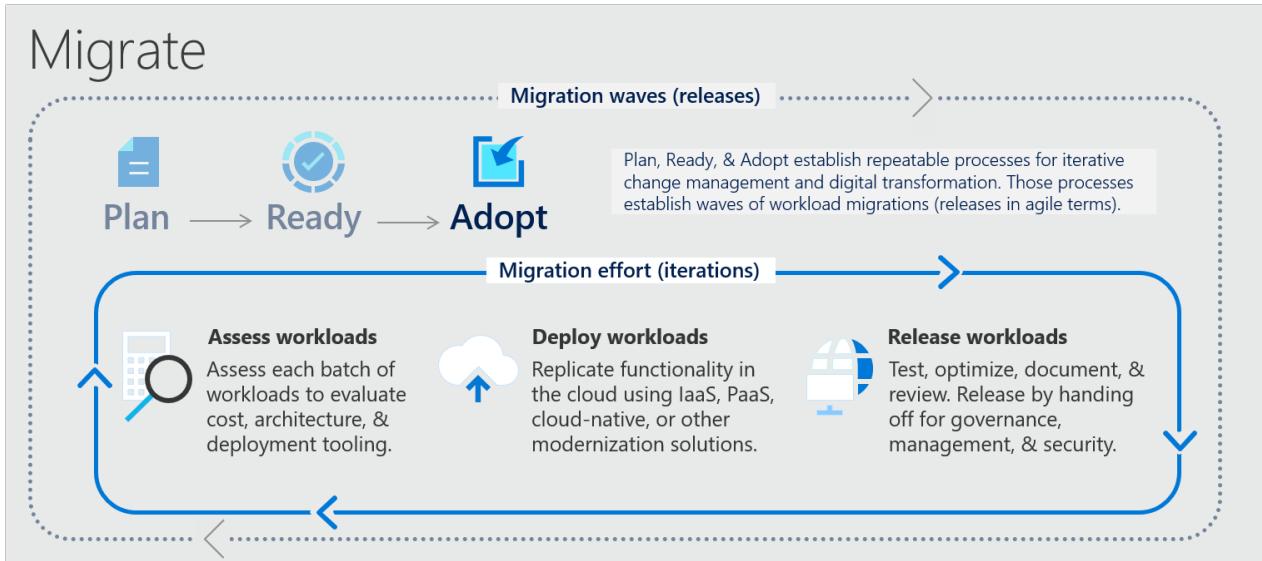


Virtual machines	Virtual machines	Linux servers	Virtual desktops
Applications	ASP.NET	Java	PHP
Data	SQL Server	Open source databases	Analytics
Hybrid	Azure Stack	VMware	
Additional scenarios	Secure workloads	Mainframes	NetApp and SAP HANA

## Migration methodology

In each of the preceding migration scenarios, the same basic process will guide your efforts as you move your

existing workloads to the cloud, as shown here:



In each scenario, you'll structure migration waves to guide the releases of multiple workloads. Establishing a cloud adoption plan and Azure landing zones through the plan and Ready methodologies helps to add structure to your migration waves.

During each iteration, follow the Migrate methodology to assess, deploy, and release workloads. To modify those processes to fit your organization's specific scenario, select any of the migration scenarios listed in the table.

## Next steps

If you aren't migrating a specific scenario, start by following the [four-step Cloud Adoption Framework migration process](#).

# Overview of application migration examples for Azure

11/9/2020 • 9 minutes to read • [Edit Online](#)

This section of the Cloud Adoption Framework for Azure provides examples of several common migration scenarios and demonstrates how you can migrate on-premises infrastructure to [Microsoft Azure](#).

## Introduction

Azure provides access to a comprehensive set of cloud services. As developers and IT professionals, you can use these services to build, deploy, and manage applications on a range of tools and frameworks through a global network of datacenters. As your business faces challenges associated with the digital shift, the Azure platform helps you to figure out how to:

- Optimize resources and operations.
- Engage with your customers and employees.
- Transform your products.

The cloud provides advantages for speed and flexibility, minimized costs, performance, and reliability. But many organizations will need to continue to run on-premises datacenters. In response to cloud adoption barriers, Azure provides a hybrid cloud strategy that builds bridges between your on-premises datacenters and the Azure public cloud. An example is using Azure cloud resources like Azure Backup to protect on-premises resources or Azure analytics to gain insights into on-premises workloads.

As part of the hybrid cloud strategy, Azure provides growing solutions for migrating on-premises applications and workloads to the cloud. With simple steps, you can comprehensively assess your on-premises resources to figure out how they'll run in the Azure platform. Then, with a deep assessment in hand, you can confidently migrate resources to Azure. When resources are up and running in Azure, you can optimize them to retain and improve access, flexibility, security, and reliability.

## Migration patterns

Strategies for migration to the cloud fall into four broad patterns: rehost, refactor, rearrange, or rebuild. The strategy you adopt depends on your business drivers and migration goals. You might adopt multiple patterns. For example, you could choose to rehost noncritical applications while rearranging applications that are more complex and business-critical. Let's look at these patterns.

PATTERN	DEFINITION	WHEN TO USE
---------	------------	-------------

Pattern	Definition	When to Use
<b>Rehost</b>	<p>Often referred to as a lift-and-shift migration, this option doesn't require code changes. You can use it to migrate your existing applications to Azure quickly. Each application is migrated as is to reap the benefits of the cloud without the risk and cost associated with code changes.</p>	<p>When you need to move applications quickly to the cloud.</p> <p>When you want to move an application without modifying it.</p> <p>When your applications are designed so that they can take advantage of <a href="#">Azure infrastructure as a service (IaaS)</a> scalability after migration.</p> <p>When applications are important to your business, but you don't need to immediately change application capabilities.</p>
<b>Refactor</b>	<p>Often referred to as "repackaging," refactoring requires minimal changes to applications so that they can connect to <a href="#">Azure platform as a service (PaaS)</a> and use cloud offerings.</p> <p>For example, you could migrate existing applications to Azure App Service or Azure Kubernetes Service (AKS).</p> <p>Or, you could refactor relational and nonrelational databases into options such as Azure SQL Managed Instance, Azure Database for MySQL, Azure Database for PostgreSQL, and Azure Cosmos DB.</p>	<p>If your application can easily be repackaged to work in Azure.</p> <p>If you want to apply innovative DevOps practices provided by Azure, or if you're thinking about DevOps using a container strategy for workloads.</p> <p>For refactoring, you need to think about the portability of your existing code base and available development skills.</p>
<b>Rearchitect</b>	<p>Rearchitecting for migration focuses on modifying and extending application functionality and the code base to optimize the application architecture for cloud scalability.</p> <p>For example, you could break down a monolithic application into a group of microservices that work together and scale easily.</p> <p>You could also rearchitect relational and nonrelational databases to a fully managed database solution, such as SQL Managed Instance, Azure Database for MySQL, Azure Database for PostgreSQL, and Azure Cosmos DB.</p>	<p>When your applications need major revisions to incorporate new capabilities or to work effectively on a cloud platform.</p> <p>When you want to use existing application investments, meet scalability requirements, apply innovative DevOps practices, and minimize use of virtual machines.</p>

PATTERN	DEFINITION	WHEN TO USE
<b>Rebuild</b>	<p>Rebuild takes things a step further by rebuilding an application from scratch using Azure cloud technologies.</p> <p>For example, you could build greenfield applications with <a href="#">cloud-native</a> technologies like Azure Functions, AI, SQL Managed Instance, and Azure Cosmos DB.</p>	<p>When you want rapid development, and existing applications have limited functionality and lifespan.</p> <p>When you're ready to expedite business innovation (including DevOps practices provided by Azure), build new applications using cloud-native technologies, and take advantage of advancements in AI, blockchain, and IoT.</p>

## Migration example articles

This section provides examples of several common migration scenarios. Each example includes background information and detailed deployment scenarios that illustrate how to set up a migration infrastructure and assess the suitability of on-premises resources for migration. More articles will be added to this section over time.

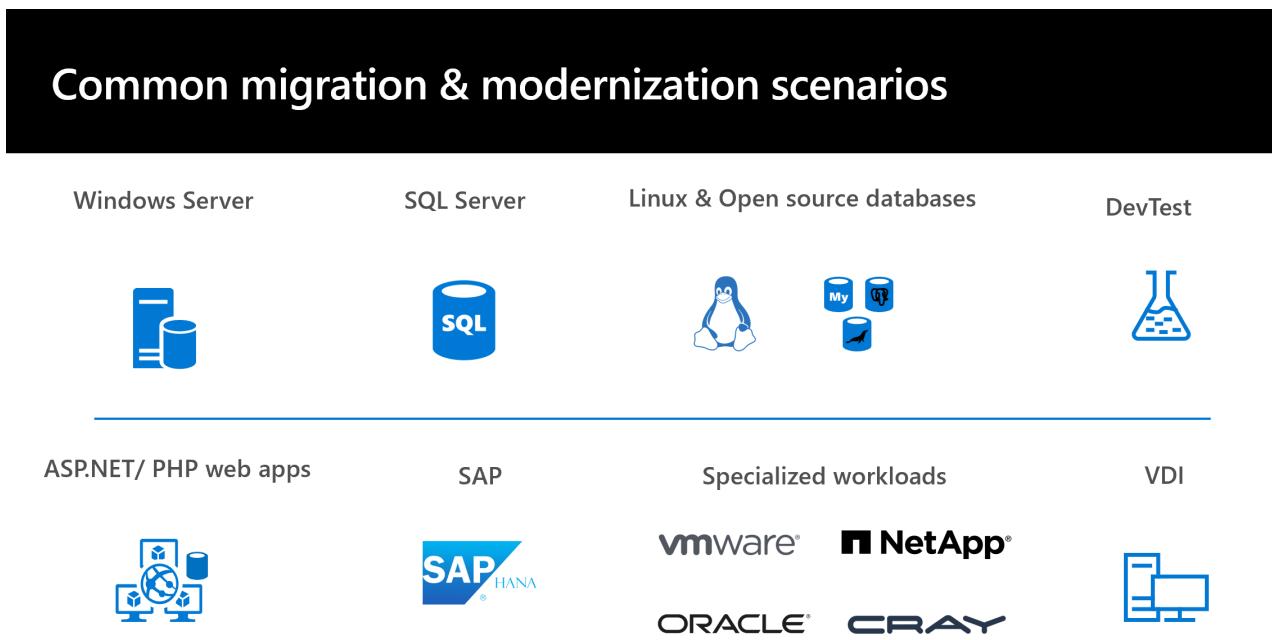


Figure 1: Common migration and modernization project categories.

This series focuses on each migration scenario, driven by slightly different business goals that determine the migration strategy. For each deployment scenario, we provide information about:

- Business drivers and goals.
- A proposed architecture.
- Steps to perform the migration.
- Recommendations for cleanup and next steps after migration is finished.

### Assessment

ARTICLE	DETAILS

ARTICLE	DETAILS
<a href="#">Assess on-premises resources for migration to Azure</a>	This best practice article in the Plan methodology discusses how to run an assessment of an on-premises application running on VMware. In the article, an example organization assesses application VMs by using Azure Migrate and the application SQL Server database by using Data Migration Assistant.

## Infrastructure

ARTICLE	DETAILS
<a href="#">Deploy Azure infrastructure</a>	This article shows how an organization can prepare its on-premises infrastructure and its Azure infrastructure for migration. The infrastructure example established in this article is referenced in the other samples provided in this section.

## Windows Server workloads

ARTICLE	DETAILS
<a href="#">Rehost an application on Azure VMs</a>	This article provides an example of migrating on-premises application VMs to Azure VMs using Azure Migrate.

## SQL Server workloads

ARTICLE	DETAILS
<a href="#">Migrate SQL Server databases to Azure</a>	This article demonstrates how the fictional company Contoso assessed, planned, and migrated its various on-premises SQL Server databases to Azure.
<a href="#">Rehost an application on an Azure VM and SQL Managed Instance</a>	This article provides an example of a lift-and-shift migration to Azure for an on-premises application. This process involves migrating the application front-end VM by using Azure Migrate and the application database to SQL Managed Instance by using <a href="#">Azure Database Migration Service</a> .
<a href="#">Rehost an application on Azure VMs using SQL Server Always On availability groups</a>	This example shows how to migrate an application and data by using Azure-hosted SQL Server VMs. It uses Azure Migrate to migrate the application VMs and Database Migration Service to migrate the application database to a SQL Server cluster that's protected by an Always On availability group.

## Linux and open-source databases

ARTICLE	DETAILS
<a href="#">Migrate open-source databases to Azure</a>	This article demonstrates how the fictional company Contoso assessed, planned, and migrated its various on-premises open-source databases to Azure.
<a href="#">Migrate MySQL to Azure</a>	This article demonstrates how the fictional company Contoso planned and migrated its on-premises MySQL open-source database platform to Azure.

ARTICLE	DETAILS
<a href="#">Migrate PostgreSQL to Azure</a>	This article demonstrates how the fictional company Contoso planned and migrated its on-premises PostgreSQL open-source database platform to Azure.
<a href="#">Migrate MariaDB to Azure</a>	This article demonstrates how the fictional company Contoso planned and migrated its on-premises MariaDB open-source database platform to Azure.
<a href="#">Rehost a Linux application on Azure VMs and Azure Database for MySQL</a>	This article provides an example of migrating a Linux-hosted application to Azure VMs by using Azure Migrate. The application database is migrated to Azure Database for MySQL by using <a href="#">Database Migration Service</a> .
<a href="#">Rehost a Linux application on Azure VMs</a>	This example shows how to complete a lift-and-shift migration of a Linux-based application to Azure VMs by using Azure Migrate.

## Dev/test workloads

ARTICLE	DETAILS
<a href="#">Migrate dev/test environments to Azure IaaS</a>	This article demonstrates how Contoso rehosts its dev/test environment for two applications running on VMware VMs by migrating to Azure VMs.
<a href="#">Migrate to Azure DevTest Labs</a>	This article discusses how Contoso moves its dev/test workloads to Azure by using DevTest Labs.

## ASP.NET and PHP web apps

ARTICLE	DETAILS
<a href="#">Refactor a Windows application using App Service and SQL Database</a>	This example shows how to migrate an on-premises Windows-based application to an Azure web app and migrate the application database to an Azure SQL Database server instance by using <a href="#">Database Migration Service</a> .
<a href="#">Refactor a Windows application using App Service and SQL Managed Instance</a>	This example shows how to migrate an on-premises Windows-based application to an Azure web app and migrate the application database to SQL Managed Instance by using <a href="#">Database Migration Service</a> .
<a href="#">Refactor a Linux application to multiple regions using App Service, Azure Traffic Manager, and Azure Database for MySQL</a>	This example shows how to migrate an on-premises Linux-based application to an Azure web app on multiple Azure regions by using Traffic Manager to integrate with GitHub for continuous delivery. The application database is migrated to an Azure Database for MySQL instance.
<a href="#">Rebuild an application in Azure</a>	This article provides an example of rebuilding an on-premises application by using a range of Azure capabilities and managed services. These capabilities and services include App Service, AKS, Azure Functions, Azure Cognitive Services, and Azure Cosmos DB.

ARTICLE	DETAILS
<a href="#">Refactor Team Foundation Server to Azure DevOps Services</a>	This article shows an example migration of an on-premises Team Foundation Server deployment to Azure DevOps Services in Azure.

## SAP

ARTICLE	DETAILS
<a href="#">SAP migration guide</a>	Get practical guidance to move your on-premises SAP workloads to the cloud.
<a href="#">Migrate SAP applications to Azure</a>	White paper and roadmap for your SAP journey to the cloud.
<a href="#">Migration methodologies for SAP on Azure</a>	Overview of various migration options to move SAP applications to Azure.

## Specialized workloads

ARTICLE	DETAILS
<a href="#">Move on-premises VMware infrastructure to Azure</a>	This article provides an example of moving on-premises VMware VMs to Azure by using Azure VMware Solution.
<a href="#">Azure NetApp Files</a>	Enterprise file storage powered by NetApp. Run Linux and Windows file workloads in Azure.
<a href="#">Oracle on Azure</a>	Run your Oracle databases and enterprise applications in Azure and Oracle Cloud Infrastructure.
<a href="#">Cray in Azure</a>	High-performance computing with Cray in Azure. A dedicated supercomputer on your virtual network.

## VDI

ARTICLE	DETAILS
<a href="#">Move on-premises Remote Desktop Services to Windows Virtual Desktop in Azure</a>	This article shows how to migrate on-premises Remote Desktop Services to Windows Virtual Desktop in Azure.

## Migration scaling

ARTICLE	DETAILS
<a href="#">Scale a migration to Azure</a>	This article shows how an example organization prepares to scale to a full migration to Azure.

## Demo applications

The example articles provided in this section use two demo applications: SmartHotel360 and osTicket.

**SmartHotel360:** This test application was developed by Microsoft to use when you work with Azure. It's provided under an open-source license, and you can download it from [GitHub](#). It's an ASP.NET application connected to a SQL Server database. In the scenarios discussed in these articles, the current version of this application is deployed to two VMware VMs running Windows Server 2008 R2 and SQL Server 2008 R2. These application VMs are hosted on-premises and managed by vCenter Server.

**osTicket**: This open-source service desk ticketing application runs on Linux. You can download it from [GitHub](#). In the scenarios discussed in these articles, the current version of this application is deployed on-premises to two VMware VMs running Ubuntu 16.04 LTS using Apache 2, PHP 7.0, and MySQL 5.7.

# Rehost an on-premises application on Azure VMs by using Azure Migrate

11/9/2020 • 13 minutes to read • [Edit Online](#)

This article demonstrates how the fictional company Contoso rehosts a two-tier Windows .NET front-end application running on VMware virtual machines (VMs) by migrating application VMs to Azure VMs.

The SmartHotel360 application used in this example is provided as open source. If you want to use it for your own testing purposes, you can download it from [GitHub](#).

## Business drivers

The IT leadership team has worked closely with business partners to understand what they want to achieve with this migration. They want to:

- **Address business growth.** Contoso is growing, so there's pressure on the company's on-premises systems and infrastructure.
- **Limit risk.** The SmartHotel360 application is critical for the Contoso business. The company wants to move the application to Azure with zero risk.
- **Extend.** Contoso doesn't want to modify the application, but it does want to ensure that the application is stable.

## Migration goals

The Contoso cloud team has pinned down goals for this migration. It used these goals to determine the best migration method:

- After migration, the application in Azure should have the same performance capabilities as it does today in VMware. The application will remain as critical in the cloud as it is on-premises.
- Although this application is important to Contoso, the company doesn't want to invest in it at this time. Contoso wants to move the application safely to the cloud in its current form.
- Contoso doesn't want to change the ops model for this application. Contoso does want to interact with it in the cloud in the same way that it does now.
- Contoso doesn't want to change any application functionality. Only the application location will change.

## Solution design

After establishing goals and requirements, Contoso designs and reviews a deployment solution. Contoso identifies the migration process, including the Azure services that it will use for the migration.

### Current application

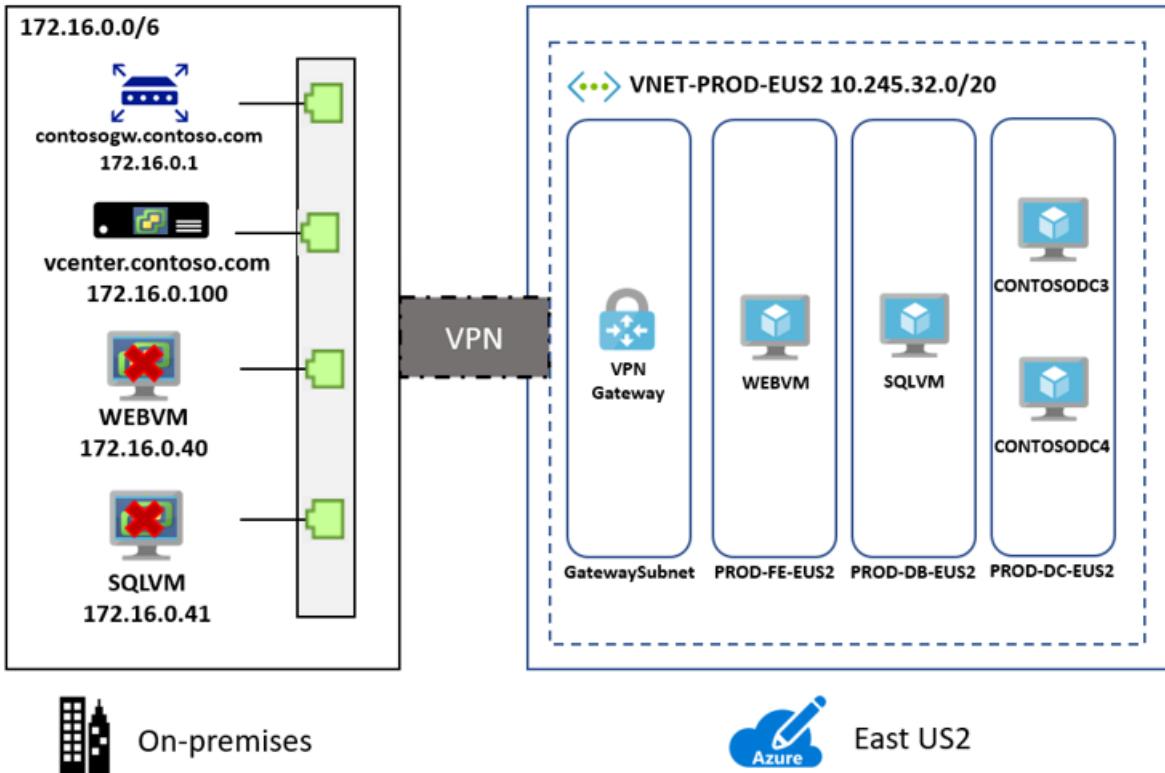
- The application is tiered across two VMs (`WEBVM` and `SQLVM`).
- The VMs are located on VMware ESXi host `contosohost1.contoso.com` (version 6.5).
- The VMware environment is managed by vCenter Server 6.5 (`vcenter.contoso.com`) running on a VM.
- Contoso has an on-premises datacenter (`contoso-datacenter`) with an on-premises domain controller (`contosodc1`).

### Proposed architecture

- Because the application is a production workload, the application VMs in Azure will reside in the production

resource group `ContosoRG`.

- The application VMs will be migrated to the primary Azure region (East US 2) and placed in the production network (`VNET-PROD-EUS2`).
- The web front-end VM will reside in the front-end subnet (`PROD-FE-EUS2`) in the production network.
- The database VM will reside in the database subnet (`PROD-DB-EUS2`) in the production network.
- The on-premises VMs in the Contoso datacenter will be decommissioned after the migration is done.



## Database considerations

As part of the solution design process, Contoso did a feature comparison between Azure SQL Database and SQL Server. The following considerations helped the company to decide to use SQL Server running on an Azure IaaS VM:

- Using an Azure VM running SQL Server seems to be an optimal solution if Contoso needs to customize the operating system and the database, or co-locate and run partner applications on the same VM.
- With Software Assurance, Contoso can later exchange existing licenses for discounted rates on Azure SQL Managed Instance by using the Azure Hybrid Benefit for SQL Server. This can save up to 30 percent on SQL Managed Instance.

## Solution review

Contoso evaluates the proposed design by putting together a list of pros and cons.

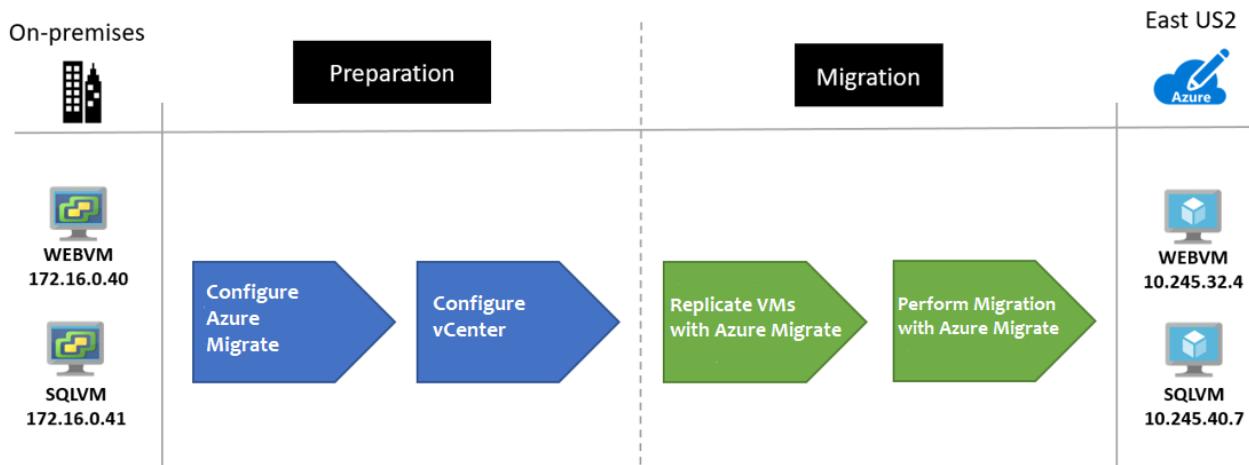
CONSIDERATION	DETAILS
---------------	---------

CONSIDERATION	DETAILS
Pros	<p>Both the application VMs will be moved to Azure without changes, making the migration simple.</p> <p>Because Contoso is using a lift-and-shift approach for both application VMs, it doesn't need any special configuration or migration tools for the application database.</p> <p>Contoso can take advantage of its investment in Software Assurance by using the Azure Hybrid Benefit.</p> <p>Contoso will retain full control of the application VMs in Azure.</p>
Cons	<p><b>WEBVM</b> and <b>SQLVM</b> are running Windows Server 2008 R2. Azure supports the operating system for specific roles. <a href="#">Learn more</a>.</p> <p>The web and data tiers of the application remain as single points of failure.</p> <p><b>SQLVM</b> is running on SQL Server 2008 R2. SQL Server 2008 R2 is no longer in mainstream support, but it is supported for Azure VMs. <a href="#">Learn more</a>.</p> <p>Contoso must continue supporting the application on Azure VMs rather than moving to a managed service such as Azure App Service or Azure SQL Database.</p>

## Migration process

Contoso will migrate the application front-end and database VMs to Azure VMs by using the agentless method in the Azure Migrate: Server Migration tool.

- As a first step, Contoso prepares and sets up Azure components for Azure Migrate: Server Migration, and prepares the on-premises VMware infrastructure.
- The [Azure infrastructure](#) is in place, so Contoso just needs to configure the replication of the VMs through the Azure Migrate: Server Migration tool.
- With everything prepared, Contoso can start replicating the VMs.
- After replication is enabled and working, Contoso will migrate the VM by testing the migration and failing it over to Azure, if successful.



## Azure services

Service	Description	Cost
Azure Migrate: Server Migration	The service orchestrates and manages migration of on-premises applications and workloads and Amazon Web Services (AWS)/Google Cloud Platform (GCP) VM instances.	During replication to Azure, Azure Storage charges are incurred. Azure VMs are created, and incur charges, when the migration occurs and the VMs are running in Azure. Learn more about <a href="#">charges and pricing</a> .

## Prerequisites

Contoso and other users must meet the following prerequisites for this scenario.

Requirements	Details
Azure subscription	<p>Contoso created subscriptions in an earlier article in this series. If you don't have an Azure subscription, create a <a href="#">free account</a>.</p> <p>If you create a free account, you're the administrator of your subscription and can perform all actions.</p> <p>If you use an existing subscription and you're not the administrator, work with the admin to assign you Owner or Contributor permissions.</p> <p>If you need more granular permissions, see <a href="#">Manage Site Recovery access with Azure role-based access control</a>.</p>
Azure infrastructure	<p>Learn how Contoso <a href="#">set up an Azure infrastructure</a>.</p> <p>Learn more about specific <a href="#">prerequisites</a> for Azure Migrate: Server Migration.</p>
On-premises servers	<p>On-premises vCenter servers should be running version 5.5, 6.0, 6.5, or 6.7.</p> <p>ESXi hosts should run version 5.5, 6.0, 6.5, or 6.7.</p> <p>One or more VMware VMs should be running on the ESXi host.</p>

## Scenario steps

Here's how Contoso admins will run the migration:

- **Step 1: Prepare Azure for Azure Migrate: Server Migration.** They add the server migration tool to their Azure Migrate project.
- **Step 2: Replicate on-premises VMs.** They set up replication and start replicating VMs to Azure Storage.
- **Step 3: Migrate the VMs with Azure Migrate: Server Migration.** They run a test migration to make sure everything's working, and then run a full migration to move the VMs to Azure.

## Step 1: Prepare Azure for Azure Migrate: Server Migration

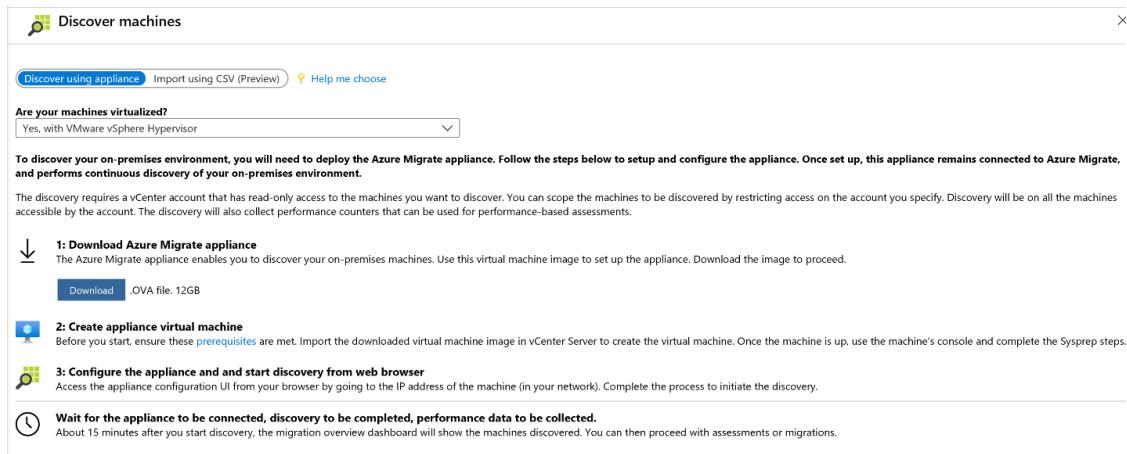
To migrate the VMs to Azure, Contoso needs a virtual network in which Azure VMs will be located when they're created during migration. It also needs the Azure Migrate: Server Migration tool (OVA file) provisioned and configured.

1. Set up a network. Contoso already set up one that can be used for Azure Migrate: Server Migration when it deployed the Azure infrastructure.

- The SmartHotel360 application is a production application, and the VMs will be migrated to the Azure production network ( VNET-PROD-EUS2 ) in the primary region ( East US 2 ).
- Both VMs will be placed in the ContosoRG resource group, which is used for production resources.
- The application front-end VM ( WEBVM ) will migrate to the front-end subnet ( PROD-FE-EUS2 ) in the production network.
- The application database VM ( SQLVM ) will migrate to the database subnet ( PROD-DB-EUS2 ) in the production network.

2. Provision the Azure Migrate: Server Migration tool.

- a. From Azure Migrate, download the OVA image and import it into VMware.



- b. Start the imported image and configure the tool, including the following steps:

- Set up the prerequisites.

## Set up discovery for Azure Migrate

Azure Migrate appliance helps you discover, assess and migrate your VMware virtual machines. Complete the following steps to initiate discovery. [Learn more](#) about Azure Migrate discovery capabilities.



### Set up prerequisites

Verify and set up appliance prerequisites



Accept license terms

[View terms of use](#)



Use of the Azure Migrate Appliance (the "software") is licensed to you as part of your or your company's subscription for the Azure Migrate Service (the "service"). Your use of the software is governed by the agreement under which you or your company obtained the service (see [Azure Legal Information](#)). Microsoft assumes no responsibility or liability whatsoever for any non-Microsoft product made available to you through your use of the service or software. Customer is solely responsible for any non-Microsoft product that it installs or uses with the service or software and acknowledges that use shall be governed by the separate agreement(s) between Customer and the publisher of the non-Microsoft product. See [TPN](#) for third-party components included in the software.



Check connectivity to the Internet

[Set up proxy](#)



Check time is in sync with the Internet time server



Check if latest Azure Migrate updates are installed



Install VMware vSphere Virtual Disk Development Kit

[Continue](#)



### Register with Azure Migrate

Specify your Microsoft Azure account details



- Point the tool to the Azure subscription.

**Set up discovery for Azure Migrate**

Azure Migrate appliance helps you discover, assess and migrate your VMware virtual machines. Complete the following steps to initiate discovery. [Learn more](#) about Azure Migrate discovery capabilities.

**Set up prerequisites**

Verify and set up appliance prerequisites

**Register with Azure Migrate**

Specify your Microsoft Azure account details



Choose the subscription and resource group that you used to set up Azure Migrate. The discovery and assessment metadata will be stored in the geography you selected while setting up Azure Migrate on the Azure portal. [Learn more](#)

Logged in as [REDACTED]

[Logout](#)

Subscription

Migrate project

Enter Appliance Name



[Register](#)

[Continue](#)

- Set the VMware vCenter credentials.

**Specify vCenter Server**

Provide vCenter Server details to discover machines. You can also choose to provide VM credentials for discovery of applications and dependencies.



Specify vCenter Server details and credentials

vCenter Server name/IP

192.168.102.91

Port

443

User name

administrator@

Password

\*\*\*\*\*

[Validate connection](#)

Successfully connected to vCenter Server

*What metadata is discovered and what is it used for? [Learn more](#)*

- Add any Windows-based credentials for discovery.

Discover applications and dependencies on VMs

Provide VM credentials for discovery of applications and for dependency analysis on the machines.

Ensure 'Guest Operations' privileges are enabled for these VMs. [Learn more](#) about permissions.

The credentials will be saved on the appliance in an encrypted format. The discovery of applications and dependencies is done remotely without the installation of any agent or script on VMs.

[Add credentials](#)

Skip addition of VM credentials. You will not be able to discover applications and dependencies.  
Added credentials

OS Type	Friendly Name	Action
Windows	basic	<a href="#">Edit</a>
Linux	basic-linux	<a href="#">Edit</a>

[Save and start discovery](#)

When you complete the configuration, the tool will take some time to enumerate all the VMs. You'll see them populate the Azure Migrate tool in Azure when this process finishes.

#### Need more help?

Learn about how to set up the [Azure Migrate: Server Migration tool](#).

#### Prepare on-premises VMs

After migration, Contoso wants to connect to the Azure VMs and allow Azure to manage the VMs. The Contoso admins must do the following steps before migration:

1. For access over the internet:

- Enable RDP or SSH on the on-premises VM before migration.
- Ensure that TCP and UDP rules are added for the **Public** profile.
- Check that RDP or SSH is allowed in the operating system firewall.

2. For access over site-to-site VPN:

- Enable RDP or SSH on the on-premises VM before migration.
- Check that RDP or SSH is allowed in the operating system firewall.
- For Windows, set the operating system's SAN policy on the on-premises VM to **OnlineAll**.

3. Install the [Azure Windows agent](#).

Other considerations:

- For Windows, there should be no Windows updates pending on the VM when you're triggering a migration. If there are, the admins won't be able to log in to the VM until the updates finish.
- After migration, the admins can check **Boot diagnostics** to view a screenshot of the VM. If this doesn't work, they should verify that the VM is running and review [troubleshooting tips](#).

#### Need more help?

Learn about how to [prepare VMs for migration](#).

## Step 2: Replicate the on-premises VMs

Before the Contoso admins can run a migration to Azure, they need to set up and enable replication.

With discovery completed, they can begin replication of VMware VMs to Azure.

1. In the Azure Migrate project, go to **Servers > Azure Migrate: Server Migration**. Then select **Replicate**.

The screenshot shows the Azure Migrate - Servers dashboard. On the left, there's a sidebar with options like Overview, Migration goals (selected), Servers, Databases, Data Box, Manage, Discovered items, Support + troubleshooting, and New support request. The main area has two sections: **Assessment tools** and **Migration tools**. The **Assessment tools** section contains a summary of discovered servers (442), groups (2), assessments (2), and notifications (0). It also includes a note: "Next step: Start migrating your servers or optionally you can refine your application grouping with dependency analysis". Below this is a link to "Add more assessment tools? Click here.". The **Migration tools** section contains a summary of discovered servers (442) and includes tabs for Discover, Replicate (which is highlighted with a red box), Migrate, and Overview. The Replicate tab is currently selected.

2. In **Replicate > Source settings > Are your machines virtualized?**, select Yes, with VMware vSphere.
3. In **On-premises appliance**, select the name of the Azure Migrate appliance that you set up, and then select OK.

The screenshot shows the "Replicate" dialog box. At the top, it says "Source settings" (which is underlined, indicating it's the active tab). Other tabs include Virtual machines, Target settings, Compute, Disks, and Review + Start replication. Below the tabs, there's a note: "The first step in migrating servers is to replicate them. Once replication completes, you can perform test migration before finally moving the servers to Azure." There are two required fields:

- \* Are your machines virtualized? (with a help icon): A dropdown menu shows "Yes, with VMware vSphere".
- \* On-premises appliance (with a help icon): A dropdown menu shows "<appliance-name>".

4. In **Virtual machines**, select the machines that you want to replicate.

- If you've run an assessment for the VMs, you can apply VM sizing and disk type (premium or standard) recommendations from the assessment results. To do this, in **Import migration settings from an Azure Migrate assessment?**, select the **Yes** option.
- If you didn't run an assessment, or you don't want to use the assessment settings, select the **No** option.
- If you selected to use the assessment, select the VM group and assessment name.

The screenshot shows the 'Replicate' wizard interface. At the top, there are tabs: 'Source settings', 'Virtual machines' (which is underlined, indicating it's the active tab), 'Target settings', 'Compute', 'Disks', and 'Review + Start replication'. Below the tabs, a section titled 'Select the virtual machines to be migrated.' contains a note about importing migration settings from an Azure Migrate assessment. A dropdown menu is open, showing two options: 'Yes, apply migration settings from a Azure Migrate assessment' (selected) and 'No, I'll specify the migration settings manually'.

5. In **Virtual machines**, search for VMs as needed and check each VM that you want to migrate. Then select **Next: Target settings**.
6. In **Target settings**, select the subscription and target region to which you'll migrate. Then specify the resource group in which the Azure VMs will reside after migration. In **Virtual Network**, select the Azure virtual network or subnet to which the Azure VMs will be joined after migration.
7. In **Azure Hybrid Benefit**:
  - Select **No** if you don't want to apply Azure Hybrid Benefit. Then select **Next**.
  - Select **Yes** if you have Windows Server machines that are covered with active Software Assurance or Windows Server subscriptions and you want to apply the benefit to the machines that you're migrating. Then select **Next**.
8. In **Compute**, review the VM name, size, OS disk type, and availability set. VMs must conform with [Azure requirements](#).
  - **VM size:** If you're using assessment recommendations, the VM size drop-down list will contain the recommended size. Otherwise, Azure Migrate picks a size based on the closest match in the Azure subscription. Alternatively, pick a manual size in **Azure VM size**.
  - **OS disk:** Specify the OS (boot) disk for the VM. The OS disk has the operating system bootloader and installer.
  - **Availability set:** If the VM should be in an Azure availability set after migration, specify the set. The set must be in the target resource group that you specify for the migration.
9. In **Disks**, specify whether the VM disks should be replicated to Azure, and select the disk type (standard SSD/HDD or premium-managed disks) in Azure. Then select **Next**.
 

You can exclude disks from replication. If you exclude disks, they won't be present on the Azure VM after migration.
10. In **Review and start replication**, review the settings, and then select **Replicate** to start the initial replication for the servers.

#### **NOTE**

You can update replication settings at any time before replication starts, in **Manage > Replicating machines**. Settings can't be changed after replication starts.

## Step 3: Migrate the VMs with Azure Migrate: Server Migration

The Contoso admins run a quick test migration and then a full migration to migrate the VMs.

### Run a test migration

1. In Migration goals > Servers > Azure Migrate: Server Migration, select Test migrated servers.

The screenshot shows the 'Migration tools' interface for Azure Migrate: Server Migration. At the top, there are four navigation tabs: Discover, Replicate, Migrate, and Overview. The 'Migrate' tab is selected. Below the tabs, there is a summary table with four rows:

Category	Count
Discovered servers	442
Replicating servers	6
<b>Test migrated servers</b>	1
Migrated servers	1

At the bottom of the dashboard, there is a note: **Next step:** You can start migrating the replicating servers to Azure.

2. Select and hold (or right-click) the VM to test, and then select **Test migrate**.

The screenshot shows the 'Replicating machines' list view in the Azure Migrate portal. On the left, there is a sidebar with navigation links: Dashboard, Azure Migrate - Servers, Azure Migrate: Server Migration - Replicating machines, Overview, Getting started, Migrate servers to Azure, Manage, Replicating machines, Jobs, Events, Settings, and Properties. The 'Replicating machines' link is selected. The main area displays a table with one row:

NAME	STATUS	HEALTH	MIGRATION PHASE	LAST SYNC	TEST MIGRATION STATUS
Contoso-Win2K8R2SP1	Delta sync	Healthy	Test migration pending	2/17/2019, 12:00:43 AM	Never performed

A context menu is open over the first row, listing options: Pin to dashboard, Test migrate (which is highlighted with a red box), Clean up test migration, and Migrate.

3. In **Test Migration**, select the Azure virtual network in which the Azure VM will be located after the migration. We recommend that you use a nonproduction virtual network.
4. The **Test migration** job starts. Monitor the job in the portal notifications.
5. After the migration finishes, view the migrated Azure VM in **Virtual Machines** in the Azure portal. The machine name has a **-Test** suffix.
6. After the test is done, select and hold (or right-click) the Azure VM in **Replicating machines**, and then select **Clean up test migration**.

Migration status					
Last refreshed at: 2/17/2019, 1:02:40 AM					
Name	Status	Health	Migration Phase	Last Sync	Test Migration Status
Contoso-Win2K8R2SP1	Delta sync	Healthy	Test clean up pending	2/17/2019, 12:00:43 AM	2/17/2019, 12:00:43 AM
<span style="float: right;">...</span> <div style="border: 1px solid #ccc; padding: 5px; margin-top: 5px;"> <span style="color: #0078d4; font-weight: bold;">Pin to dashboard</span>   <span style="color: #0078d4; font-weight: bold;">Test migrate</span>   <span style="color: red; font-weight: bold;">Clean up test migration</span>   <span style="color: #0078d4; font-weight: bold;">Migrate</span>   <span style="color: #0078d4; font-weight: bold;">Error Details</span> </div>					

## Migrate the VMs

Now the Contoso admins run a full migration.

- In the Azure Migrate project, select Servers > Azure Migrate: Server Migration > Replicating servers.

Category	Count
Discovered servers	58
Replicating servers	1
Test migrated servers	0
Migrated servers	0

**Next step:** You can start migrating the replicating servers to Azure

- In Replicating machines, select and hold (or right-click) the VM, and then select **Migrate**.
- In **Migrate** > **Shut down virtual machines and perform a planned migration with no data loss**, select **Yes** > **OK**.

By default, Azure Migrate shuts down the on-premises VM and runs an on-demand replication to synchronize any VM changes that occurred since the last replication. This ensures no data loss. If you don't want to shut down the VM, select **No**.

- A migration job starts for the VM. Track the job in Azure notifications.
- After the job finishes, you can view and manage the VM from the **Virtual Machines** page.

## Need more help?

- Learn about how to [run a test migration](#).
- Learn about how to [migrate VMs to Azure](#).

## Clean up after migration

With migration complete, the SmartHotel360 application tiers are now running on Azure VMs.

Now, Contoso needs to do these cleanup steps:

- After the migration is complete, stop replication.
- Remove the **WEBVM** machine from the vCenter inventory.
- Remove the **SQLVM** machine from the vCenter inventory.
- Remove **WEBVM** and **SQLVM** from local backup jobs.
- Update internal documentation to show the new location and IP addresses for the VMs.
- Review any resources that interact with the VMs, and update any relevant settings or documentation to reflect the new configuration.

## Review the deployment

With the application now running, Contoso needs to fully operationalize and secure it in Azure.

### Security

The Contoso security team reviews the Azure VMs to determine any security issues. To control access, the team reviews the network security groups (NSGs) for the VMs. NSGs are used to ensure that only traffic allowed to the application can reach it. The team also considers securing the data on the disk by using Azure Disk Encryption and Key Vault.

For more information, see [Security best practices for IaaS workloads in Azure](#).

## Business continuity and disaster recovery

For business continuity and disaster recovery, Contoso takes the following actions:

- Keep data safe: Contoso [backs up the data on the VMs by using Azure Backup](#).
- Keep applications up and running: Contoso [replicates the application VMs in Azure to a secondary region by using Azure Site Recovery](#).

### Licensing and cost optimization

Contoso has existing licensing for its VMs and will take advantage of the Azure Hybrid Benefit. Contoso will convert the existing Azure VMs to take advantage of this pricing.

Contoso will enable [Azure Cost Management and Billing](#) to help monitor and manage Azure resources.

## Conclusion

In this article, Contoso rehosted the SmartHotel360 application in Azure. The admins migrated the application VMs to Azure VMs by using the Azure Migrate: Server Migration tool.

# Migrate SQL Server databases to Azure

11/9/2020 • 10 minutes to read • [Edit Online](#)

This article demonstrates how a fictional company Contoso assessed, planned and migrated their various on-premises SQL Server databases to Azure.

As Contoso considers migrating to Azure, the company needs a technical and financial assessment to determine whether its on-premises workloads are good candidates for cloud migration. In particular, the Contoso team wants to assess machine and database compatibility for migration. Additionally, it wants to estimate capacity and costs for running Contoso's resources in Azure.

## Business drivers

Contoso is having various issues with maintaining all the wide array of versions of SQL Server workloads that exist on their network. After the latest investor's meeting, the CFO and CTO have made the decision to move all these workloads to Azure. This will allow them to shift from a structured capital expense model to a fluid operating expense model.

The IT leadership team has worked closely with business partners to understand the business and technical requirements:

- **Increase security:** Contoso needs to be able to monitor and protect all data resources in a more timely and efficient manner. They would also like to get a more centralized reporting system setup on database access patterns.
- **Optimize compute resources:** Contoso has deployed a large on-premises server infrastructure. They have several SQL Server instances that consume but do not really use the underlying CPU, memory and disk allocated in efficient ways.
- **Increase efficiency:** Contoso needs to remove unnecessary procedures, and streamline processes for developers and users. The business needs IT to be fast and not waste time or money, thus delivering faster on customer requirements. Database administration should be reduced and/or minimized after the migration.
- **Increase agility:** Contoso IT needs to be more responsive to the needs of the business. It must be able to react faster than the changes in the marketplace, to enable the success in a global economy. It mustn't get in the way, or become a business blocker.
- **Scale:** As the business grows successfully, Contoso IT must provide systems that are able to grow at the same pace. There are several legacy hardware environments that cannot be upgraded any further and are past or near end of support.
- **Costs:** Business and applications owners want to know they won't be stuck with high cloud costs as compared to running the applications on-premises.

## Migration goals

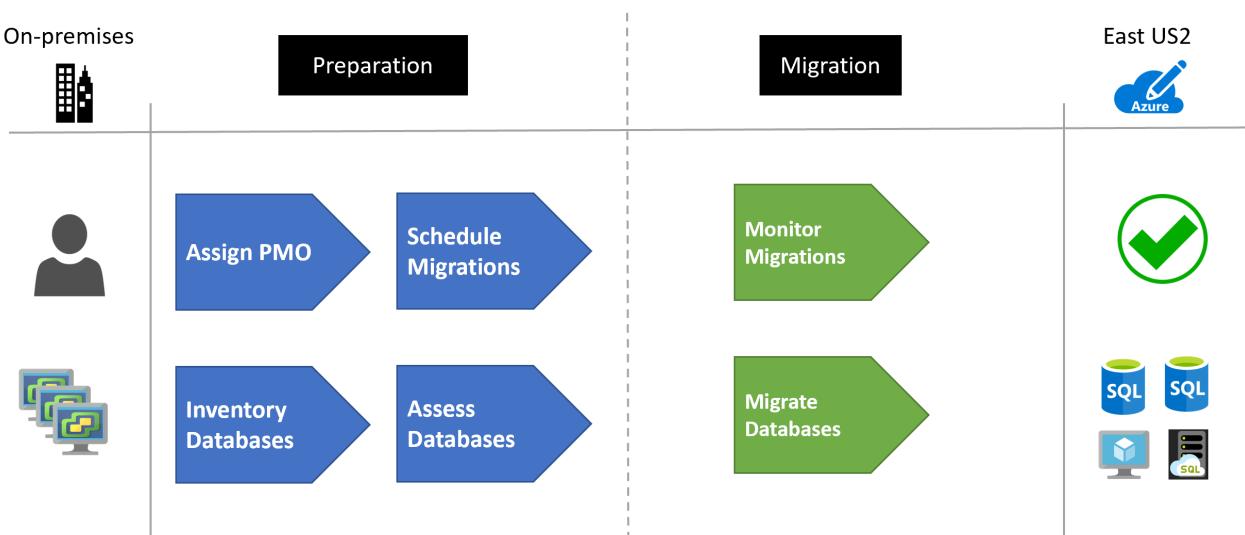
The Contoso cloud team has pinned down goals for the various migrations. These goals were used to determine the best migration methods.

Requirements	Details
<b>Performance</b>	After migration, applications in Azure should have the same performance capabilities that applications have today in Contoso's on-premises environment. Moving to the cloud doesn't mean that application performance is less critical.
<b>Compatibility</b>	Contoso needs to understand the compatibility of its applications and databases with Azure. Contoso also needs to understand its Azure hosting options.
<b>Data sources</b>	All databases will be moved to Azure with no exceptions. Based on the database and application analysis of the SQL features being used, they will move to PaaS, IaaS or managed instances. All databases must move.
<b>Application</b>	Applications must be moved to the cloud wherever possible. If they cannot move, then they will be allowed to connect to the migrated database over the Azure network through private connections only.
<b>Costs</b>	Contoso wants to understand not only its migration options, but also the costs associated with the infrastructure after it moves to the cloud.
<b>Management</b>	Resource management groups must be created for the various departments along with resource groups to manage all SQL databases that are migrated. All resources must be tagged with department information for charge-back requirements.
<b>Limitations</b>	Initially, not all branch offices that run applications will have a direct ExpressRoute link to Azure, so these offices will need to connect through virtual network gateways.

## Solution design

Contoso has already performed a [migration assessment](#) of their digital estate using [Azure Migrate](#).

The assessment results in multiple workloads spread across multiple departments. The overall size of the migration project will require a full project management office (PMO), to manage the specifics of communication, resources and schedule planning.



## Solution review

Contoso evaluates their proposed design by putting together a pros and cons list.

CONSIDERATION	DETAILS
Pros	Azure will provide a single pane of glass into the database workloads  Costs will be monitored via Azure Cost Management and Billing.  Business charge-back billing will be easy to perform with the Azure Billing APIs.  Server and software maintenance will be reduced to only the IaaS-based environments.
Cons	Due to the requirement of IaaS-based virtual machines, there will still need to be management of the software on those machines.

## Budget and management

Before the migration can occur, the necessary Azure structure is required to be in place to support the administration and billing aspects of the solution.

For the management requirements, several [management groups](#) were created to support the organizational structure.

For the billing requirements, each of the Azure resources are then [tagged](#) with the appropriate billing tags.

## Migration process

Data migrations follow a standard repeatable pattern. This involves the following steps based on [Microsoft best practices](#):

- Pre-migration:
  - **Discovery:** Inventory database assets and application stack.
  - **Assess:** Assess workloads and fix recommendations.
  - **Convert:** Convert source schema to work in the target.
- Migration:
  - **Migrate:** Migrate the source schema, source data and objects to target.
  - **Sync data:** Sync data (for minimal downtime).
  - **Cutover:** Cut over the source to target.
- Post-migration:
  - **Remediate applications:** Iteratively make and necessary changes to your applications.
  - **Perform tests:** Iteratively run functional and performance tests.
  - **Optimize:** Based on tests, address performance issues and then retest to confirm performance improvements.
  - **Retire assets:** Old VMs and hosting environments are backed up and retired.

### Step 1: Discovery

Contoso used Azure Migrate to surface the dependencies across the Contoso environment. Azure Migrate automatically discovered application components on Windows and Linux systems and mapped the communication between services. Azure Migrate also surfaced the connections between Contoso servers, processes, inbound and outbound connection latency, and ports across their TCP-connected architecture.

Contoso also added Data Migration Assistant to their Azure Migrate project. By selecting this tool they're able to assess the databases for migration to Azure.

[Home](#) > [Azure Migrate | Databases](#) >

## Add a tool

[Select assessment tool](#)   [Select migration tool](#)   [Review + add tool\(s\)](#)

will be used to store discovery, assessment and migration metadata reported by the on-premises environment. [Learn more](#)

Start by choosing a database assessment tool. We recommend that you assess your datacenter to determine migration readiness.

Tool	Pricing	Supported Workloads	Features
 <b>Azure Migrate: Database Assessment</b>	Free	SQL Server 2005 - 2017	Target and size Readiness assessment Compatibility analysis Schema conversion

### Step 2: Application assessment

The results from the assessment provided Contoso with the visibility that they utilize mainly .NET-based applications, however, over the years various projects have used other technologies such as PHP and Node.js. Vendor purchased systems also introduced non-.NET-based applications. They have identified the following:

- ~800 Windows .NET applications
- ~50 PHP applications
- 25 Node.js applications
- 10 Java applications

### Step 3: Database assessment

As each database workload was discovered, Data Migration Assistant (DMA) tool was run to determine which features were being used. DMA helps Contoso assess their database migrations to Azure by detecting compatibility issues that can impact database functionality in a new version of SQL Server or Azure SQL Database.

Contoso followed these steps to assess their databases and then upload results data to Azure Migrate:

1. Download DMA.
2. Create an assessment project.
3. In DMA, logon to the Azure Migrate project and sync the assessment summary.

# Assess databases

X

The Data Migration Assistant (DMA) helps you assess your database migration to Azure by detecting compatibility issues that can impact database functionality in your new version of SQL Server or Azure SQL Database. DMA recommends performance and reliability improvements for your target environment and allows you to move your schema, data, and uncontained objects from your source server to your target server.

**To assess your on-premises databases, you need to download the Data Migration Assistant tool (DMA). Follow the steps below to download and install DMA. Once installed, DMA will assess your on-premises databases and upload results to an Azure Migrate Project.**



## 1: Download DMA

Download DMA and get the Azure target, size and comprehensive assessment report migrating to Azure Databases.

[Download](#)



## 2: Create an Assessment project



Create an assessment project in DMA by providing the source server type, intended Azure target type to get the feature parity and database compatibility assessments.



## 3: In DMA logon to Azure Migrate Project and sync assessment summary

In DMA, log on to the Azure, select the Azure Migrate project and upload the summary results of the assessments.

DMA recommends performance and reliability improvements for your target environment and allows them to move their schema, data, and uncontained objects from a source server to a target server.

Learn more about [Data Migration Assistant](#)

Contoso used the DMA to run the assessment and then uploaded the data directly to Azure Migrate.

Feature parity (2)	
Recommendation	Impacted o...
<b>Unsupported features (2)</b>	
Azure SQL Database does not sup...	1
Windows authentication not supp...	N/A
Partially-supported features (0)	

Azure SQL Database does not support trace flags

Details		Impacted objects	
Impact		Type	Name
Trace flags are used to temporarily set specific server characteristics or to switch off a particular behavior. Trace flags are frequently used to diagnose performance issues or to debug stored procedures or complex computer systems.		Trace flag	8017
Recommendation		Object details	
Choose the right SQL Database service tiers and performance level for single databases and elastic databases that match your workloads.		Type: Trace flag Name: 8017	

[Upload to Azure Migrate](#)



With the database information now loaded into Azure Migrate, Contoso has identified over 1,000 database instances that must be migrated. Of these instances, roughly 40 percent can be moved to SQL Database for Azure. The remaining 60 percent must be moved either to either SQL Server running on Azure Virtual Machines or to Azure SQL Managed Instance. Of those 60 percent, about 10 percent require a virtual machine-based approach, the remaining instances will be moved to Azure SQL Managed Instance.

When DMA was not able to be executed on a data source, the following guidelines were followed on the database migrations.

**NOTE**

As part of the Assess phase, Contoso discovered various open source databases. Separately, they followed [Migrate open-source databases to Azure](#) for their migration planning.

**Step 4: Migration planning**

With the information at hand, Contoso uses the following guidelines to determine which migration method to use for each database.

TARGET	DATABASE USAGE	DETAILS	ONLINE MIGRATION	OFFLINE MIGRATION	MAX SIZE	MIGRATION GUIDE
Azure SQL Database (PaaS)	SQL Server (data only)	These databases simply use basic tables, columns, stored procedures and functions	Data Migration Assistant, transactional replication	BACPAC, bcp	1 TiB	<a href="#">Link</a>
Azure SQL Managed Instance	SQL Server (advanced features)	These databases use triggers and other <a href="#">advanced concepts</a> such as custom .NET types, service brokers, etc.	Data Migration Assistant, transactional replication	BACPAC, bcp, native backup/restore	2 TiB - 8 TiB	<a href="#">Link</a>

Target	Database Usage	Details	Online Migration	Offline Migration	Max Size	Migration Guide
SQL Server on Azure Virtual Machines (IaaS)	SQL Server (third-party integrations)	The SQL Server must have <a href="#">non-supported SQL Managed Instance features</a> (cross-instance service brokers, cryptographic providers, buffer pool, compatibility levels below 100, database mirroring, FILESTREAM, PolyBase, anything that requires access to file shares, external scripts, extended stored procedures, and others) or third-party software installed to support the activities of the database.	<a href="#">transactional replication</a>	<a href="#">BACPAC</a> , <a href="#">bcp</a> , <a href="#">snapshot replication</a> , <a href="#">native backup/restore</a> , <a href="#">convert physical machine to VM</a>	4 GiB - 64 TiB	<a href="#">Link</a>

Due to the large number of databases, Contoso created a project management office (PMO) to keep track of every database migration instance. [Accountability and responsibilities](#) were assigned to each business and application team.

Contoso also performed a [workload readiness review](#). This review examined the infrastructure, database and network components.

#### Step 5: Test migrations

The first part of the migration preparation involved a test migration of each of the databases to the pre-setup environments. In order to save time, they scripted all of the operations for the migrations and recorded the timings for each. In order to speed up the migration, they identified what migration operations could be run concurrently.

Any rollback procedures were identified for each of the database workloads in case of some unexpected failures.

For the IaaS-based workloads, they set up all the required third-party software beforehand.

After the test migration, Contoso was able to use the various Azure [cost estimation tools](#) to get a more accurate picture of the future operational costs of their migration.

#### Step 6: Migration

For the production migration, Contoso identified the time frames for all database migrations and what could be sufficiently executed in a weekend window (midnight Friday through midnight Sunday) with minimal downtime to

the business.

Based on their documented test procedures, they execute each migration via scripting as much as possible, limiting any manual tasks to minimize errors.

If any migrations fail during the window, they're rolled back and re-scheduled in the next migration window.

### Clean up after migration

Contoso identified the archival window for all database workloads. As the window expires, the resources will be retired from the on-premises infrastructure.

This includes:

- Removing the production data from on-premises servers.
- Retiring the hosting server when the last workload window expires.

### Review the deployment

With the migrated resources in Azure, Contoso needs to fully operationalize and secure their new infrastructure.

#### Security

- Contoso needs to ensure that their new Azure database workloads are secure. [Learn more](#).
- In particular, Contoso should review the firewall and virtual network configurations.
- Setup [Private Link](#) so that all database traffic is kept inside Azure and the on-premises network.
- Enable [Azure Advanced Threat Protection](#) for Azure SQL Database.

#### Backups

- Ensure that the Azure databases are backed up using geo-restore. This allows backups to be used in a paired region in case of a regional outage.
- **Important:** Ensure that the Azure resource has a [resource lock](#) to prevent it from being deleted. Deleted servers cannot be restored.

#### Licensing and cost optimization

- Many Azure database workloads can be scaled up or down, therefore performance monitoring of the server and databases is important to ensure you're meeting your needs but also keeping costs at a minimum.
- Both CPU and storage have costs associated. There are several pricing tiers to select from. Be sure the appropriate pricing plan is selected for the data workloads.
- [Elastic pools](#) are to be implemented for databases that have compatible resource utilization patterns.
- Each read replica is billed based on the compute and storage selected
- Use reserved capacity to save on costs.

## Conclusion

In this article, Contoso assessed, planned and migrated their Microsoft SQL Server workloads to Azure.

# Rehost an on-premises application by migrating to Azure VMs and Azure SQL Managed Instance

11/9/2020 • 26 minutes to read • [Edit Online](#)

This article shows how the fictional company Contoso migrates a two-tier Windows .NET front-end application running on VMware virtual machines (VMs) to an Azure VM by using Azure Migrate. It also shows how Contoso migrates the application database to Azure SQL Managed Instance.

The SmartHotel360 application used in this example is provided as open source. If you want to use it for your own testing purposes, download it from [GitHub](#).

## Business drivers

Contoso's IT leadership team has worked closely with the company's business partners to understand what the business wants to achieve with this migration. They want to:

- **Address business growth.** Contoso is growing. As a result, pressure has increased on the company's on-premises systems and infrastructure.
- **Increase efficiency.** Contoso needs to remove unnecessary procedures and streamline processes for its developers and users. The business needs IT to be fast and not waste time or money for the company to deliver faster on customer requirements.
- **Increase agility.** Contoso IT needs to be more responsive to the needs of the business. It must react faster than the changes that occur in the marketplace for the company to be successful in a global economy. IT at Contoso must not get in the way or become a business blocker.
- **Scale.** As the company's business grows successfully, Contoso IT must provide systems that can grow at the same pace.

## Migration goals

The Contoso cloud team has identified goals for this migration. The company uses migration goals to determine the best migration method.

- After migration, the application in Azure should have the same performance capabilities that the application has today in Contoso's on-premises VMware environment. Moving to the cloud doesn't mean that application performance is less critical.
- Contoso doesn't want to invest in the application. The application is critical and important to the business, but Contoso simply wants to move the application in its current form to the cloud.
- Database administration tasks should be minimized after the application is migrated.
- Contoso doesn't want to use Azure SQL Database for this application. It's looking for alternatives.

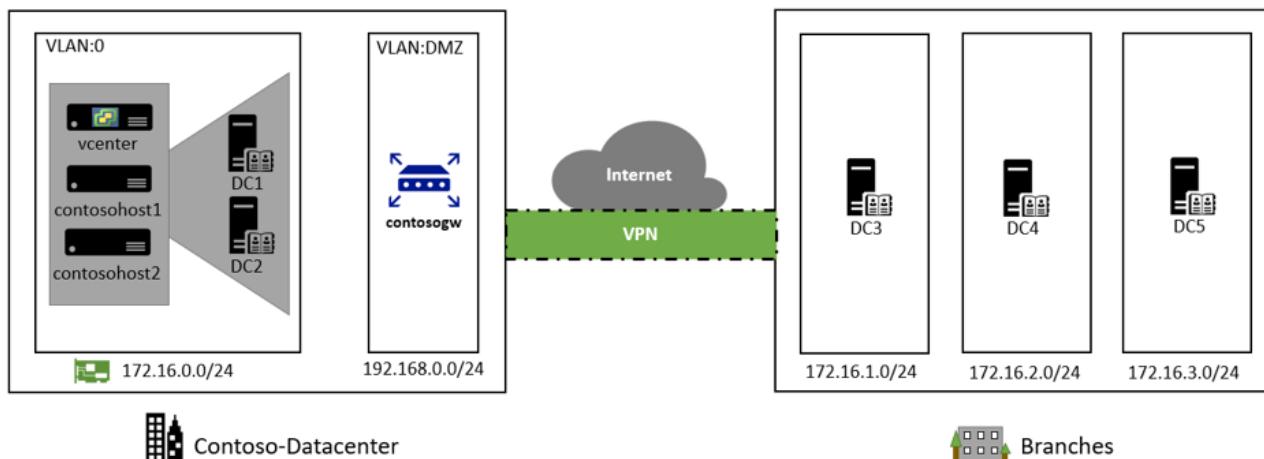
## Solution design

After pinning down the company's goals and requirements, Contoso designs and reviews a deployment solution and identifies the migration process. The Azure services that it will use for the migration also are identified.

### Current architecture

- Contoso has one main datacenter ( `contoso-datacenter` ). The datacenter is located in New York City in the eastern United States.
- Contoso has three additional local branches across the United States.

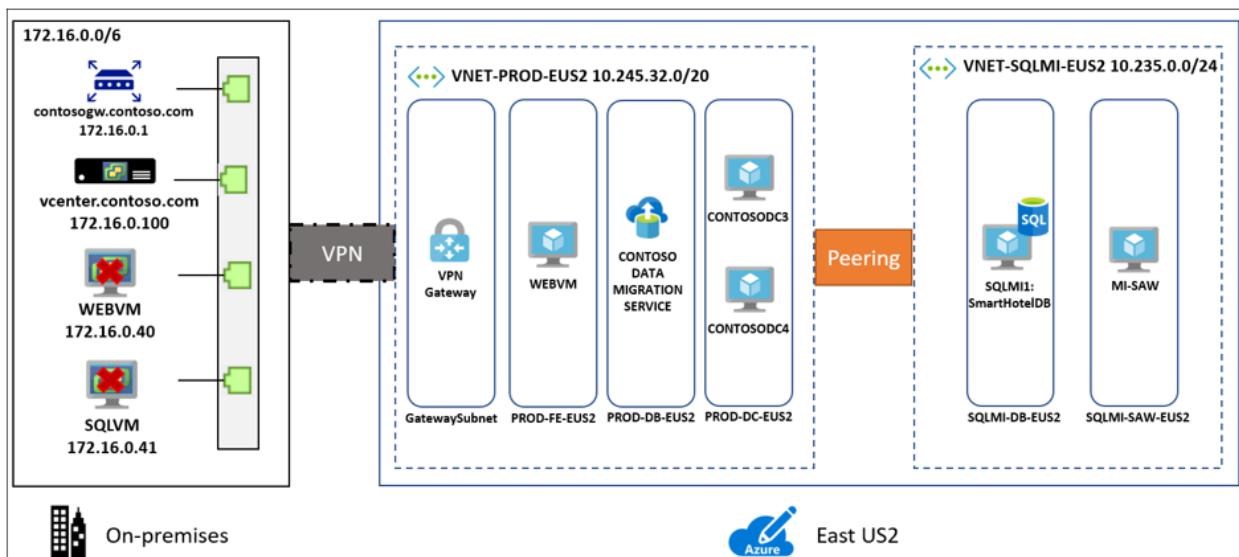
- The main datacenter is connected to the internet with a fiber-optic Metro Ethernet connection (500 megabits per second).
- Each branch is connected locally to the internet by using business-class connections with IPsec VPN tunnels back to the main datacenter. The setup allows Contoso's entire network to be permanently connected and optimizes internet connectivity.
- The main datacenter is fully virtualized with VMware. Contoso has two ESXi 6.5 virtualization hosts that are managed by vCenter Server 6.5.
- Contoso uses Active Directory for identity management. Contoso uses DNS servers on the internal network.
- Contoso has an on-premises domain controller (`contosodc1`).
- The domain controllers run on VMware VMs. The domain controllers at local branches run on physical servers.
- The SmartHotel360 application is tiered across two VMs (`WEBVM` and `SQLVM`) that are located on a VMware ESXi version 6.5 host (`contosohost1.contoso.com`).
- The VMware environment is managed by vCenter Server 6.5 (`vcenter.contoso.com`) running on a VM.



## Proposed architecture

In this scenario, Contoso wants to migrate its two-tier on-premises travel application as follows:

- Migrate the application database (`SmartHotelDB`) to a SQL managed instance.
- Migrate the front end, `WEBVM`, to an Azure VM.
- The on-premises VMs in the Contoso datacenter will be decommissioned when the migration is finished.



## Database considerations

As part of the solution design process, Contoso did a feature comparison between Azure SQL Database and SQL

Managed Instance. The following considerations helped the company decide to use SQL Managed Instance.

- SQL Managed Instance aims to deliver almost 100% compatibility with the latest on-premises SQL Server version. We recommend SQL Managed Instance for customers who are running SQL Server on-premises or on infrastructure as a service (IaaS) VMs and want to migrate their applications to a fully managed service with minimal design changes.
- Contoso is planning to migrate a large number of applications from on-premises to IaaS. Many of these applications are ISV provided. Contoso realizes that using SQL Managed Instance will help ensure database compatibility for these applications, rather than using SQL Database, which might not be supported.
- Contoso can perform a lift-and-shift migration to SQL Managed Instance by using the fully automated Azure Database Migration Service. With this service in place, Contoso can reuse it for future database migrations.
- SQL Managed Instance supports SQL Server Agent, an important component of the SmartHotel360 application. Contoso needs this compatibility. Otherwise, it will have to redesign maintenance plans required by the application.
- With Software Assurance, Contoso can exchange its existing licenses for discounted rates on a SQL managed instance by using the Azure Hybrid Benefit for SQL Server. For this reason, Contoso can save up to 30 percent on SQL Managed Instance.
- SQL Managed Instance is fully contained in the virtual network, so it provides greater isolation and security for Contoso's data. Contoso can get the benefits of the public cloud while keeping the environment isolated from the public internet.
- SQL Managed Instance supports many security features. They include Always Encrypted, dynamic data masking, row-level security, and threat detection.

## Solution review

Contoso evaluates the proposed design by putting together a list of pros and cons.

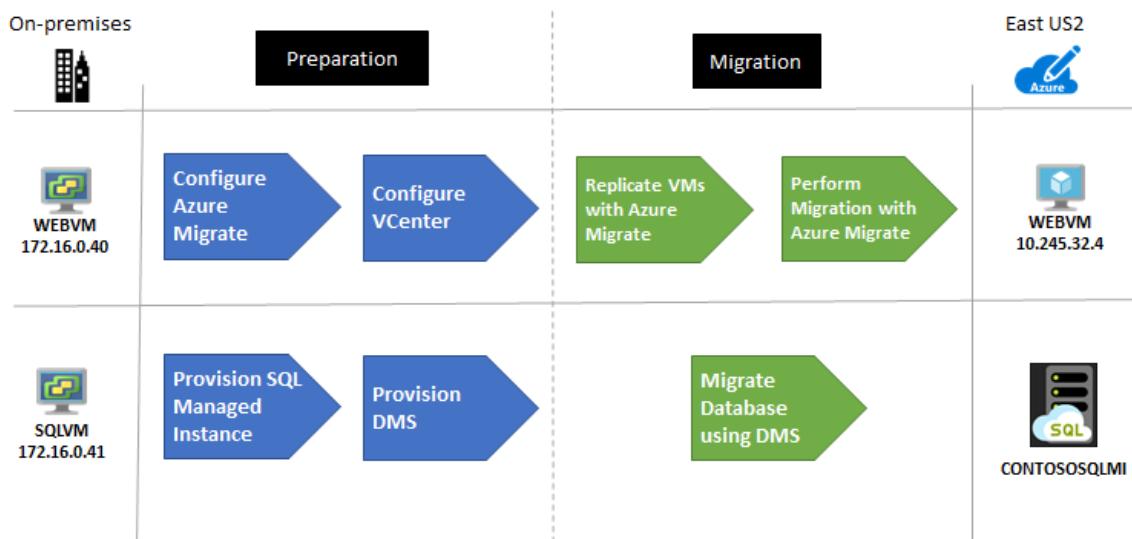
CONSIDERATION	DETAILS
Pros	<p>WEBVM will be moved to Azure without changes, which makes the migration simple.</p> <p>SQL Managed Instance supports Contoso's technical requirements and goals.</p> <p>SQL Managed Instance will provide 100 percent compatibility with Contoso's current deployment while moving the company away from SQL Server 2008 R2.</p> <p>Contoso can take advantage of its investment in Software Assurance and use the Azure Hybrid Benefit for SQL Server and Windows Server.</p> <p>Contoso can reuse Azure Database Migration Service for additional future migrations.</p> <p>SQL Managed Instance has built-in fault tolerance that Contoso doesn't need to configure. This feature ensures that the data tier is no longer a single point of failure.</p>

CONSIDERATION	DETAILS
Cons	<p><b>WEBVM</b> is running Windows Server 2008 R2. Although this operating system is supported by Azure, it's no longer a supported platform. To learn more, see <a href="#">Support policy for Microsoft SQL Server products</a>.</p> <p>The web tier remains a single point of failover with only <b>WEBVM</b> providing services.</p> <p>Contoso will need to continue supporting the application web tier as a VM rather than moving to a managed service, such as Azure App Service.</p> <p>For the data tier, SQL Managed Instance might not be the best solution if Contoso wants to customize the operating system or the database server, or if the company wants to run third-party applications along with SQL Server. Running SQL Server on an IaaS VM could provide this flexibility.</p>

## Migration process

Contoso will migrate the web and data tiers of its SmartHotel360 application to Azure by completing these steps:

1. Contoso already has its Azure infrastructure in place, so it just needs to add a couple of specific Azure components for this scenario.
2. The data tier will be migrated by using Azure Database Migration Service. This service connects to the on-premises SQL Server VM across a site-to-site VPN connection between the Contoso datacenter and Azure. The service then migrates the database.
3. The web tier will be migrated by using a lift-and-shift migration by using Azure Migrate. The process entails preparing the on-premises VMware environment, setting up and enabling replication, and migrating the VMs by failing them over to Azure.



## Azure services

SERVICE	DESCRIPTION	COST

Service	Description	Cost
Azure Database Migration Service	Azure Database Migration Service enables seamless migration from multiple database sources to Azure data platforms with minimal downtime.	Learn about <a href="#">supported regions</a> and <a href="#">Azure Database Migration Service pricing</a> .
Azure SQL Managed Instance	SQL Managed Instance is a managed database service that represents a fully managed SQL Server instance in the Azure cloud. It uses the same code as the latest version of SQL Server Database Engine and has the latest features, performance improvements, and security patches.	Using a SQL managed instance running in Azure incurs charges based on capacity. Learn more about <a href="#">SQL Managed Instance pricing</a> .
Azure Migrate	Contoso uses Azure Migrate to assess its VMware VMs. Azure Migrate assesses the migration suitability of the machines. It provides sizing and cost estimates for running in Azure.	Azure Migrate is available at no additional charge. They might incur charges depending on the tools (first-party or independent software vendor) they decide to use for assessment and migration. Learn more about <a href="#">Azure Migrate pricing</a> .

## Prerequisites

Contoso and other users must meet the following prerequisites for this scenario.

Requirements	Details
Azure subscription	<p>Contoso already created a subscription in the first article in this series. If you don't have an Azure subscription, create a <a href="#">free account</a>.</p> <p>If you create a free account, you're the administrator of your subscription and can perform all actions.</p> <p>If you use an existing subscription and you're not the administrator of the subscription, work with the admin to assign you Owner or Contributor permissions to the necessary resource groups and resources.</p>
Azure infrastructure	Contoso set up its Azure infrastructure as described in <a href="#">Azure infrastructure for migration</a> .
On-premises servers	<p>The on-premises vCenter Server should be running version 5.5, 6.0, or 6.5.</p> <p>An ESXi host should be running version 5.5, 6.0, or 6.5.</p> <p>One or more VMware VMs should be running on the ESXi host.</p>
On-premises VMs	<a href="#">Review Linux machines</a> that are endorsed to run on Azure.

Requirements	Details
<b>Database Migration Service</b>	<p>For Azure Database Migration Service, you need a <a href="#">compatible on-premises VPN device</a>.</p> <p>You must be able to configure the on-premises VPN device. It must have an external-facing public IPv4 address. The address can't be located behind a NAT device.</p> <p>Make sure you can access your on-premises SQL Server database.</p> <p>Windows Firewall should be able to access the source database engine. Learn how to <a href="#">configure Windows Firewall for database engine access</a>.</p> <p>If there's a firewall in front of your database machine, add rules to allow access to the database and files via SMB port 445.</p> <p>The credentials that are used to connect to the source SQL Server instance and that target SQL Managed Instance must be members of the sysadmin server role.</p> <p>You need a network share in your on-premises database that Azure Database Migration Service can use to back up the source database.</p> <p>Make sure that the service account running the source SQL Server instance has write permissions on the network share.</p> <p>Make a note of a Windows user and password that has full control permissions on the network share. Azure Database Migration Service impersonates these user credentials to upload backup files to the Azure Storage container.</p> <p>The SQL Server Express installation process sets the TCP/IP protocol to <b>Disabled</b> by default. Make sure that it's enabled.</p>

## Scenario steps

Here's how Contoso plans to set up the deployment:

- **Step 1: Prepare a SQL managed instance.** Contoso needs an existing managed instance to which the on-premises SQL Server database will migrate.
- **Step 2: Prepare Azure Database Migration Service.** Contoso must register the database migration provider, create an instance, and then create a Database Migration Service project. Contoso also must set up a shared access signature (SAS) uniform resource identifier (URI) for the Database Migration Service instance. An SAS URI provides delegated access to resources in Contoso's storage account so that Contoso can grant limited permissions to storage objects. Contoso sets up an SAS URI so that Azure Database Migration Service can access the storage account container to which the service uploads the SQL Server backup files.
- **Step 3: Prepare Azure for the Azure Migrate: Server Migration tool.** Contoso adds the server migration tool to its Azure Migrate project.
- **Step 4: Prepare on-premises VMware for Azure Migrate: Server Migration.** Contoso prepares accounts for VM discovery and prepares to connect to Azure VMs after migration.
- **Step 5: Replicate the on-premises VMs.** Contoso sets up replication and starts replicating VMs to Azure Storage.
- **Step 6: Migrate the database via Azure Database Migration Service.** Contoso migrates the database.

- **Step 7: Migrate the VMs with Azure Migrate: Server Migration.** Contoso runs a test migration to make sure everything's working and then runs a full migrate to move the VM to Azure.

## Step 1: Prepare a SQL managed instance

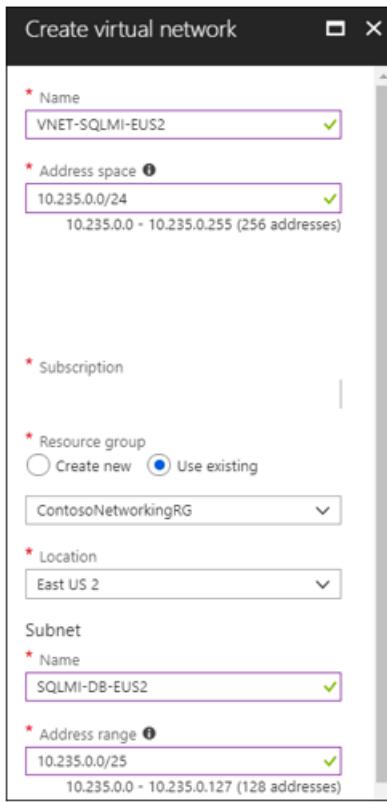
To set up a SQL managed instance, Contoso needs a subnet that meets the following requirements:

- The subnet must be dedicated. It must be empty. It can't contain any other cloud service. The subnet can't be a gateway subnet.
- After the managed instance is created, Contoso shouldn't add resources to the subnet.
- The subnet can't have a network security group associated with it.
- The subnet must have a user-defined route table. The only route assigned should be `0.0.0.0/0` next-hop internet.
- If an optional custom DNS is specified for the virtual network, the virtual IP address `168.63.129.16` for the recursive resolvers in Azure must be added to the list. Learn how to [configure custom DNS for a SQL managed instance](#).
- The subnet must not have a service endpoint (storage or SQL) associated with it. Service endpoints should be disabled on the virtual network.
- The subnet must have a minimum of 16 IP addresses. Learn how to [size the managed instance subnet](#).
- In Contoso's hybrid environment, custom DNS settings are required. Contoso configures DNS settings to use one or more of the company's Azure DNS servers. Learn more about [DNS customization](#).

### Set up a virtual network for the managed instance

To set up the virtual network, the Contoso admins:

1. Create a new virtual network (`VNET-SQLMI-EU2`) in the primary region (`East US 2`). It adds the virtual network to the `ContosoNetworkingRG` resource group.
2. Assign an address space of `10.235.0.0/24`. They ensure that the range doesn't overlap with any other networks in its enterprise.
3. Add two subnets to the network:
  - `SQLMI-DS-EUS2` (`10.235.0.0/25`).
  - `SQLMI-SAW-EUS2` (`10.235.0.128/29`). This subnet is used to attach a directory to the managed instance.



4. After the virtual network and subnets are deployed, they peer networks as follows:

- Peers **VNET-SQLMI-EUS2** with **VNET-HUB-EUS2** (the hub virtual network in **East US 2**).
- Peers **VNET-SQLMI-EUS2** with **VNET-PROD-EUS2** (the production network).

NAME	PEERING STATUS	PEER
VNET-SQLMI-EUS2-to-VNET-PROD-EUS2	Connected	VNET-PROD-EUS2
VNET-SQLMI-EUS2-to-VNET-HUB-EUS2	Connected	VNET-HUB-EUS2

5. Set custom DNS settings. DNS points first to Contoso's Azure domain controllers. Azure DNS is secondary.

The Contoso Azure domain controllers are located as follows:

- Located in the **PROD-DC-EUS2** subnet, in the **East US 2** production network (**VNET-PROD-EUS2**).
- CONTOSODC3** address: **10.245.42.4**.
- CONTOSODC4** address: **10.245.42.5**.
- Azure DNS resolver: **168.63.129.16**.

The screenshot shows the 'DNS servers' section of the Azure portal for a specific virtual network. The 'Custom' option is chosen, and three custom DNS servers are listed with their IP addresses. An 'Add DNS server' button is available for adding more.

## Need more help?

- Read the [SQL Managed Instance overview](#).
- Learn how to [create a virtual network for a SQL managed instance](#).
- Learn how to [set up peering](#).
- Learn how to [update Azure Active Directory DNS settings](#).

## Set up routing

The managed instance is placed in a private virtual network. Contoso needs a route table for the virtual network to communicate with the Azure management service. If the virtual network can't communicate with the service that manages it, the virtual network becomes inaccessible.

Contoso considers these factors:

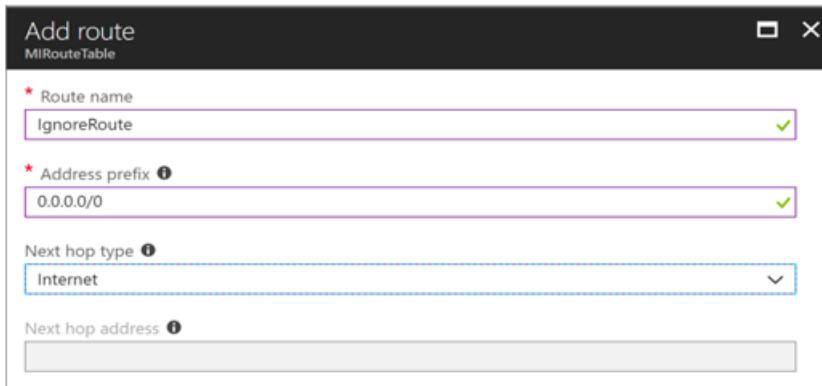
- The route table contains a set of rules (routes) that specify how packets sent from the managed instance should be routed in the virtual network.
- The route table is associated with subnets where managed instances are deployed. Each packet that leaves a subnet is handled based on the associated route table.
- A subnet can be associated with only one route table.
- There are no additional charges for creating route tables in Microsoft Azure.

To set up routing, the Contoso admins do the following steps:

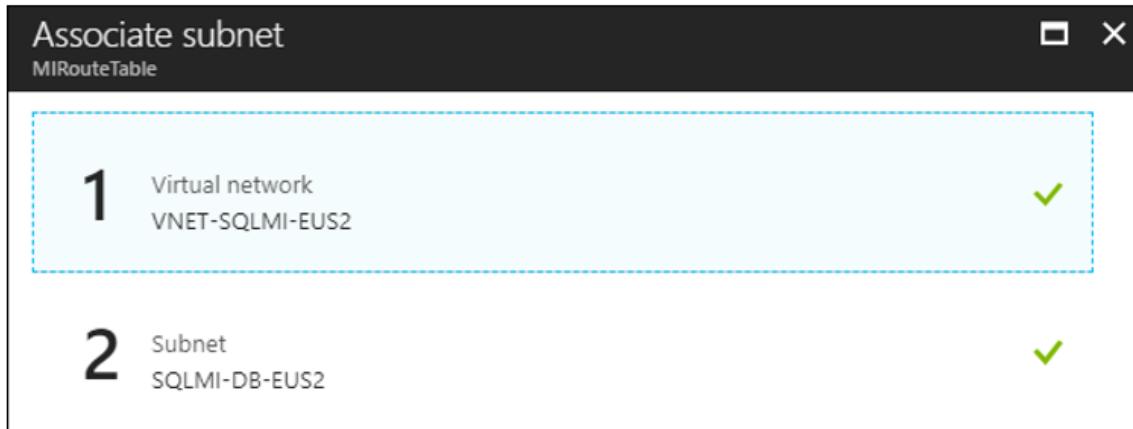
1. Create a user-defined route table in the `ContosoNetworkingRG` resource group.

The dialog box for creating a route table. It includes fields for Name (MIRouteTable), Subscription, Resource group (ContosoNetworkingRG), Location (East US 2), and BGP route propagation (Disabled).

2. To comply with SQL Managed Instance requirements, after the route table (`MIRouteTable`) is deployed, they add a route that has an address prefix of `0.0.0.0/0`. The **Next hop type** option is set to **Internet**.



3. Associate the route table with the `SQLMI-DB-EUS2` subnet (in the `VNET-SQLMI-EUS2` network).



## Need more help?

Learn how to [set up routes for a managed instance](#).

## Create a managed instance

Now the Contoso admins can provision a SQL managed instance:

1. Because the managed instance serves a business application, they deploy the managed instance in the company's primary region (`East US 2`). They add the managed instance to the `ContosoRG` resource group.
2. They select a pricing tier, size compute, and storage for the instance. Learn more about [SQL Managed Instance pricing](#).

SQL Managed Instance

\* Subscription  
<subscription id>

Preview terms  
Accepted

\* Managed instance name  
contososqlmi

\* Managed instance admin login  
contosoadmin

\* Password  
.....

\* Confirm password  
.....

\* Resource group i  
 Create new  Use existing  
ContosoRG

\* Location i  
East US 2

\* Virtual network i  
VNET-SQLMI-EUS2/SQLMI-DB-EUS2

3. After the managed instance is deployed, two new resources appear in the  resource group:

- The new SQL managed instance.
- A virtual cluster in case Contoso has multiple managed instances.

	NAME	TYPE	LOCATION
<input type="checkbox"/>	VirtualClusterManagedInstances	Virtual cluster	East US 2
<input type="checkbox"/>	contososqlmi	SQL managed instance	East US 2

#### Need more help?

Learn how to [provision a managed instance](#).

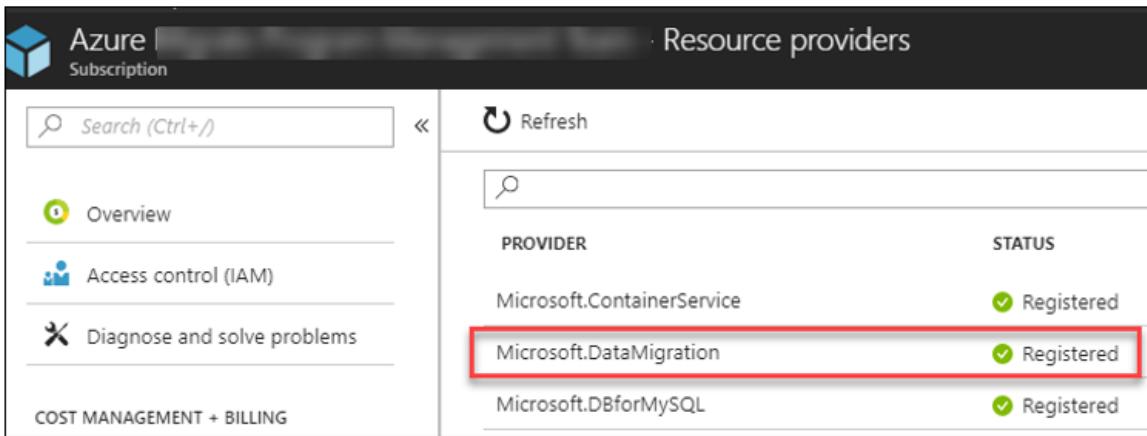
## Step 2: Prepare Azure Database Migration Service

To prepare Azure Database Migration Service, the Contoso admins need to do a few things:

- Register the Database Migration Service provider in Azure.
- Grant permission for Database Migration Service to access Azure Storage for uploading the backup files that are used to migrate a database. To provide access to Azure Storage, create an Azure Blob storage container. Generate an SAS URI for the Blob storage container.
- Create an Azure Database Migration Service project.

They complete the following steps:

1. Register the database migration provider under its subscription.



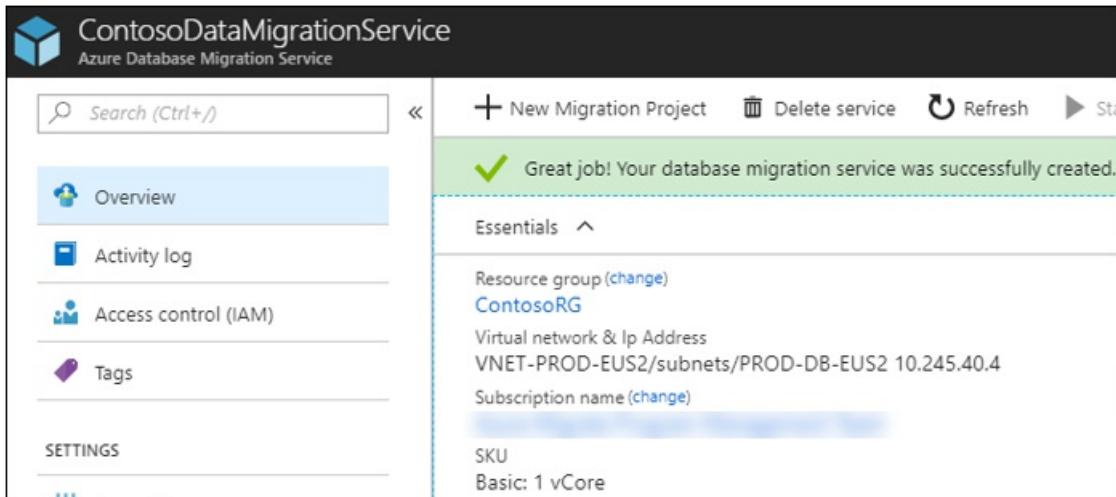
The screenshot shows the 'Resource providers' section in the Azure portal. On the left, there's a sidebar with 'Overview', 'Access control (IAM)', 'Diagnose and solve problems', and 'COST MANAGEMENT + BILLING'. The main area lists providers with their status: 'Microsoft.ContainerService' is 'Registered', 'Microsoft.DataMigration' is highlighted with a red border and is also 'Registered', and 'Microsoft.DBforMySQL' is 'Registered'.

2. Create an Azure Blob storage container. Contoso generates an SAS URI so that Azure Database Migration Service can access it.



The screenshot shows the 'Shared Access Signature' dialog in Azure Storage Explorer. It has fields for 'Container:' (set to 'datamigration'), 'URL:' (showing a blob URL), and 'Query string:' (showing a SAS token). There are 'Copy' buttons next to each field.

3. Create an Azure Database Migration Service instance.



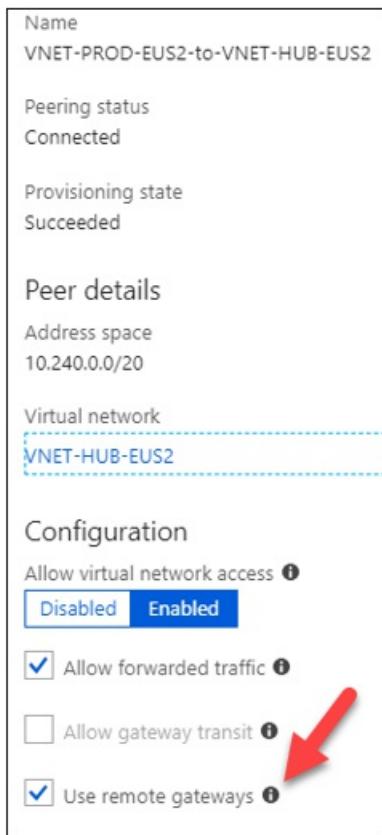
The screenshot shows the 'ContosoDataMigrationService' overview page. The sidebar includes 'Overview' (which is selected and highlighted in blue), 'Activity log', 'Access control (IAM)', and 'Tags'. The main content area displays a success message: 'Great job! Your database migration service was successfully created.' It shows details like 'Resource group (change) ContosoRG', 'Virtual network & Ip Address VNET-PROD-EUS2/subnets/PROD-DB-EUS2 10.245.40.4', 'Subscription name (change)', and 'SKU Basic: 1 vCore'.

4. Place the Database Migration Service instance in the `PROD-DC-EUS2` subnet of the `VNET-PROD-DC-EUS2` virtual network.

- The instance is placed here because the service must be in a virtual network that can access the on-

premises SQL Server VM via a VPN gateway.

- `VNET-PROD-EUS2` is peered to `VNET-HUB-EUS2` and is allowed to use remote gateways. The **Use remote gateways** option ensures that the instance can communicate as required.



#### Need more help?

- Learn how to [set up Azure Database Migration Service](#).
- Learn how to [create and use SAS](#).

## Step 3: Prepare Azure for the Azure Migrate: Server Migration tool

Here are the Azure components Contoso needs to migrate the VMs to Azure:

- A virtual network in which Azure VMs will be located when they're created during migration.
- The Azure Migrate: Server Migration tool provisioned.

The Contoso admins set up these components:

1. Set up a network. Contoso already set up a network that can be used for Azure Migrate: Server Migration when it [deployed the Azure infrastructure](#).
  - The SmarHotel360 application is a production application, and the VMs will be migrated to the Azure production network (`VNET-PROD-EUS2`) in the primary region (`East US 2`).
  - Both VMs will be placed in the `ContosoRG` resource group, which is used for production resources.
  - The application front-end VM (`WEBVM`) will migrate to the front-end subnet (`PROD-FE-EUS2`) of the production network.
  - The application database VM (`SQLVM`) will migrate to the database subnet (`PROD-DB-EUS2`) of the production network.

## Step 4: Prepare on-premises VMware for Azure Migrate: Server

# Migration

Here are the Azure components Contoso needs to migrate the VMs to Azure:

- A virtual network in which Azure VMs will be located when they're created during migration.
- The Azure Migrate appliance, provisioned and configured.

The Contoso admins set up these components by following these steps:

1. Set up a network. Contoso already set up a network that can be used for Azure Migrate: Server Migration when it [deployed the Azure infrastructure](#).
  - The SmartHotel360 application is a production application, and the VMs will be migrated to the Azure production network (`VNET-PROD-EUS2`) in the primary region (`East US 2`).
  - Both VMs will be placed in the `ContosoORG` resource group, which is used for production resources.
  - The application front-end VM (`WEBVM`) will migrate to the front-end subnet (`PROD-FE-EUS2`) in the production network.
  - The application database VM (`SQLVM`) will migrate to the database subnet (`PROD-DB-EUS2`) in the production network.
2. Provision the Azure Migrate appliance.

- a. From Azure Migrate, download the OVA image and import it into VMware.

The screenshot shows the 'Discover machines' wizard in the Azure portal. It has four main steps:

- 1: Download Azure Migrate appliance**: This step shows a download button for a 12GB .OVA file. It includes a note: "The Azure Migrate appliance enables you to discover your on-premises machines. Use this virtual machine image to set up the appliance. Download the image to proceed." A 'Download' button is available.
- 2: Create appliance virtual machine**: This step lists prerequisites and instructions: "Before you start, ensure these [prerequisites](#) are met. Import the downloaded virtual machine image in vCenter Server to create the virtual machine. Once the machine is up, use the machine's console and complete the Sysprep steps." It also includes a note: "The discovery requires a vCenter account that has read-only access to the machines you want to discover. You can scope the machines to be discovered by restricting access on the account you specify. Discovery will be on all the machines accessible by the account. The discovery will also collect performance counters that can be used for performance-based assessments."
- 3: Configure the appliance and start discovery from web browser**: This step provides instructions: "Access the appliance configuration UI from your browser by going to the IP address of the machine (in your network). Complete the process to initiate the discovery."
- 4: Wait for the appliance to be connected, discovery to be completed, performance data to be collected**: This step includes a note: "About 15 minutes after you start discovery, the migration overview dashboard will show the machines discovered. You can then proceed with assessments or migrations." It features a clock icon indicating the time frame.

- b. Start the imported image and configure the tool by following these steps:

- a. Set up the prerequisites.

## Set up discovery for Azure Migrate

Azure Migrate appliance helps you discover, assess and migrate your VMware virtual machines. Complete the following steps to initiate discovery. [Learn more](#) about Azure Migrate discovery capabilities.



### Set up prerequisites

Verify and set up appliance prerequisites



Accept license terms

[View terms of use](#)



Use of the Azure Migrate Appliance (the "software") is licensed to you as part of your or your company's subscription for the Azure Migrate Service (the "service"). Your use of the software is governed by the agreement under which you or your company obtained the service (see [Azure Legal Information](#)). Microsoft assumes no responsibility or liability whatsoever for any non-Microsoft product made available to you through your use of the service or software. Customer is solely responsible for any non-Microsoft product that it installs or uses with the service or software and acknowledges that use shall be governed by the separate agreement(s) between Customer and the publisher of the non-Microsoft product. See [TPN](#) for third-party components included in the software.



Check connectivity to the Internet

[Set up proxy](#)



Check time is in sync with the Internet time server



Check if latest Azure Migrate updates are installed



Install VMware vSphere Virtual Disk Development Kit

[Continue](#)



### Register with Azure Migrate

Specify your Microsoft Azure account details



- b. Point the tool to the Azure subscription.

**Set up discovery for Azure Migrate**

Azure Migrate appliance helps you discover, assess and migrate your VMware virtual machines. Complete the following steps to initiate discovery. [Learn more](#) about Azure Migrate discovery capabilities.

**Set up prerequisites**

Verify and set up appliance prerequisites

**Register with Azure Migrate**

Specify your Microsoft Azure account details



Choose the subscription and resource group that you used to set up Azure Migrate. The discovery and assessment metadata will be stored in the geography you selected while setting up Azure Migrate on the Azure portal. [Learn more](#)

Logged in as [REDACTED]

[Logout](#)

## Subscription

[REDACTED]

## Migrate project

[REDACTED]

## Enter Appliance Name

[REDACTED]

[Register](#)[Continue](#)

## c. Set the VMware vCenter credentials.

**Specify vCenter Server**

Provide vCenter Server details to discover machines. You can also choose to provide VM credentials for discovery of applications and dependencies.



## Specify vCenter Server details and credentials

## vCenter Server name/IP

## Port

## User name

## Password

[Validate connection](#)
✓ Successfully connected to vCenter Server

*What metadata is discovered and what is it used for? [Learn more](#)*

## d. Add any Linux-based or Windows-based credentials for discovery.

Discover applications and dependencies on VMs

Provide VM credentials for discovery of applications and for dependency analysis on the machines.

Ensure 'Guest Operations' privileges are enabled for these VMs. [Learn more](#) about permissions.

The credentials will be saved on the appliance in an encrypted format. The discovery of applications and dependencies is done remotely without the installation of any agent or script on VMs.

[Add credentials](#)

Skip addition of VM credentials. You will not be able to discover applications and dependencies.  
Added credentials

OS Type	Friendly Name	Action
Windows	basic	<a href="#">Edit</a>
Linux	basic-linux	<a href="#">Edit</a>

[Save and start discovery](#)

- After configuration, it takes some time for the tool to enumerate all the virtual machines. After the process is finished, the Contoso admins can see the VMs populated in the Azure Migrate tool in Azure.

## Need more help?

Learn about how to set up the [Azure Migrate appliance](#).

## Prepare on-premises VMs

After migration, Contoso wants to connect to the Azure VMs and allow Azure to manage the VMs. The Contoso admins must do the following steps before migration:

- For access over the internet, they:
  - Enable RDP or SSH on the on-premises VM before migration.
  - Ensure that TCP and UDP rules are added for the **Public** profile.
  - Check that RDP or SSH is allowed in the operating system firewall.
- For access over site-to-site VPN, they:
  - Enable RDP or SSH on the on-premises VM before migration.
  - Check that RDP or SSH is allowed in the operating system firewall.
  - For Windows, set the operating system's SAN policy on the on-premises VM to **OnlineAll**.
- They install the Azure agent:
  - [Azure Linux agent](#)
  - [Azure Windows agent](#)
- Other considerations:
  - For Windows, there should be no Windows updates pending on the VM when triggering a migration. If there are, they won't be able to log in to the VM until the update finishes.
  - After migration, they can check **boot diagnostics** to view a screenshot of the VM. If this doesn't work, they should verify that the VM is running and review these [troubleshooting tips](#).

## Need more help?

Learn about how to [prepare VMs for migration](#).

## Step 5: Replicate the on-premises VMs

Before the Contoso admins can run a migration to Azure, they need to set up and enable replication.

With discovery completed, they can begin replication of VMware VMs to Azure.

1. In the Azure Migrate project, they go to **Servers > Azure Migrate: Server Migration**. Then they select **Replicate**.

The screenshot shows the Azure Migrate - Servers dashboard. On the left, there's a sidebar with links for Overview, Migration goals (Servers selected), Databases, Data Box, Manage (Discovered items selected), Support + troubleshooting, and New support request. The main area has two sections: **Assessment tools** and **Migration tools**. The Assessment tools section contains a summary of discovered servers (442), groups (2), assessments (2), and notifications (0). It also includes a note: "Next step: Start migrating your servers or optionally you can refine your application grouping with dependency analysis". Below this is a link to "Add more assessment tools? Click here.". The Migration tools section contains a summary of discovered servers (442) and features tabs for Discover, Replicate (which is highlighted with a red box), Migrate, and Overview. The Replicate tab is currently selected.

2. In **Replicate > Source settings > Are your machines virtualized?**, they select **Yes, with VMware vSphere**.
3. In **On-premises appliance**, they select the name of the Azure Migrate appliance that was set up and then select **OK**.

**Replicate**

---

Source settings   Virtual machines   Target settings   Compute   Disks   Review + Start replication

The first step in migrating servers is to replicate them. Once replication completes, you can perform test migration before finally moving the servers to Azure.

\* Are your machines virtualized? ⓘ  
Yes, with VMware vSphere

\* On-premises appliance ⓘ  
<onprem-appliance-name>

4. In **Virtual machines**, they select the machines they want to replicate:

- If they've run an assessment for the VMs, they can apply VM sizing and disk type (premium/standard) recommendations from the assessment results. In **Import migration settings from an Azure Migrate assessment?**, they select the **Yes** option.
- If they didn't run an assessment or they don't want to use the assessment settings, they select the **No** option.
- If they selected to use the assessment, they select the VM group and assessment name.

**Replicate**

---

Source settings   **Virtual machines**   Target settings   Compute   Disks   Review + Start replication

Select the virtual machines to be migrated.

\* Import migration settings from an assessment? ⓘ  
Select

Yes, apply migration settings from a Azure Migrate assessment  
No, I'll specify the migration settings manually

5. In **Virtual machines**, they search for VMs as needed and check each VM they want to migrate. Then they select **Next: Target settings**.

6. In **Target settings**, they select the subscription and target region to which they'll migrate. They also specify the resource group in which the Azure VMs will reside after migration. In **Virtual Network**, they select the Azure virtual network/subnet to which the Azure VMs will be joined after migration.

7. In **Azure Hybrid Benefit**, they:

- Select **No** if they don't want to apply Azure Hybrid Benefit. Then they select **Next**.
- Select **Yes** if they have Windows Server machines that are covered with active Software Assurance or Windows Server subscriptions and they want to apply the benefit to the machines they're migrating. Then they select **Next**.

8. In **Compute**, they review the VM name, size, OS disk type, and availability set. VMs must conform with [Azure requirements](#).

- **VM size:** If they're using assessment recommendations, the VM size drop-down list contains the recommended size. Otherwise, Azure Migrate picks a size based on the closest match in the Azure subscription. Alternatively, they can pick a manual size in **Azure VM size**.
- **OS disk:** They specify the OS (boot) disk for the VM. The OS disk is the disk that has the operating system bootloader and installer.
- **Availability set:** If the VM should be in an Azure availability set after migration, they specify the set. The set must be in the target resource group specified for the migration.

9. In **Disks**, they specify whether the VM disks should be replicated to Azure. Then they select the disk type (standard SSD/HDD or premium-managed disks) in Azure and select **Next**.

- They can exclude disks from replication.
- If disks are excluded, they won't be present on the Azure VM after migration.

10. In **Review + start replication**, they review the settings. Then they select **Replicate** to start the initial replication for the servers.

**NOTE**

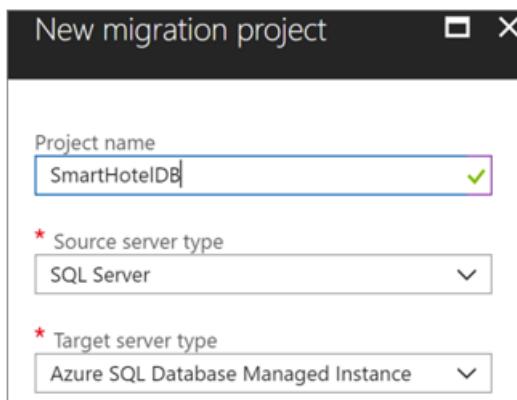
Replication settings can be updated any time before replication starts in **Manage > Replicating machines**. Settings can't be changed after replication starts.

## Step 6: Migrate the database via Azure Database Migration Service

The Contoso admins need to create a Database Migration Service project and then migrate the database.

### Create an Azure Database Migration Service project

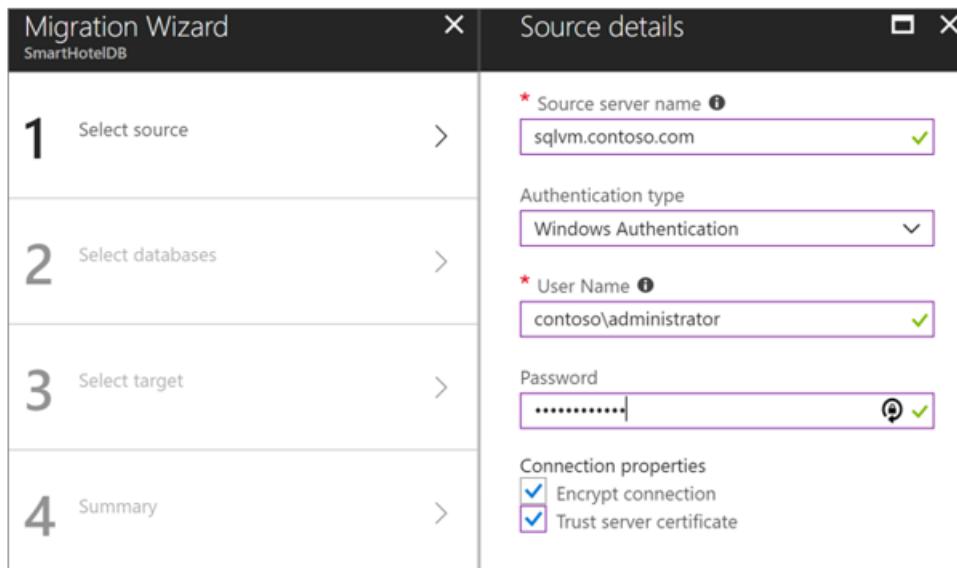
1. The admins create a Database Migration Service project. They select the **SQL Server** source server type and **Azure SQL Managed Instance** as the target.



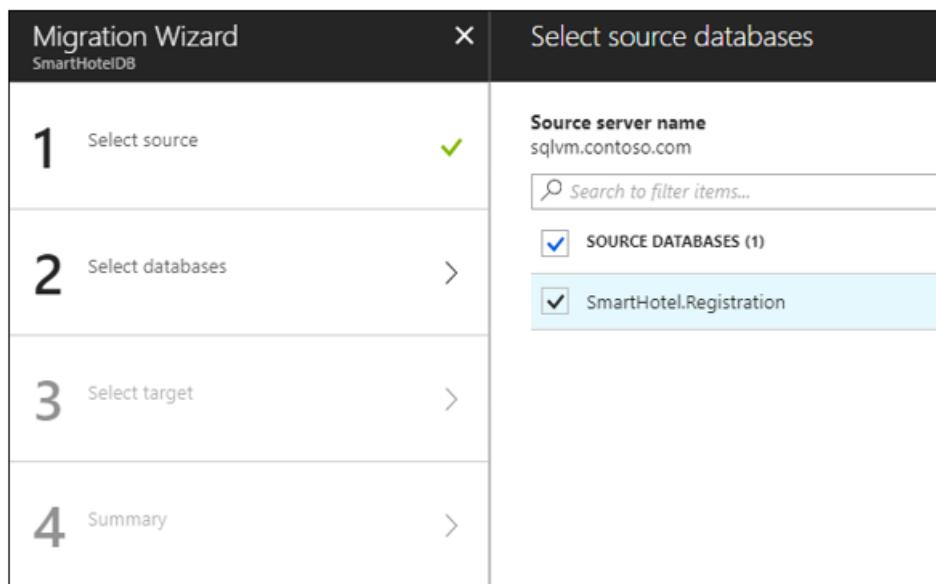
2. The Migration Wizard opens.

### Migrate the database

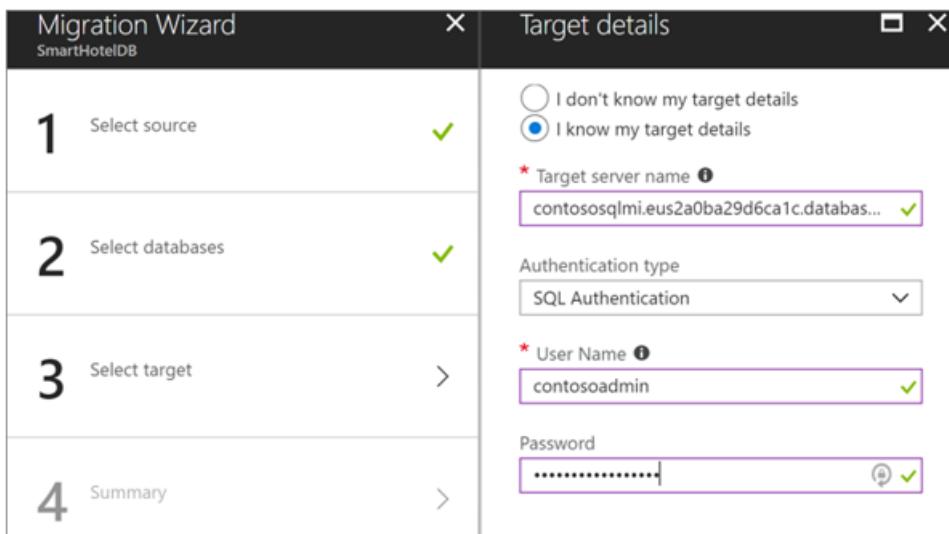
1. In the Migration Wizard, they specify the source VM on which the on-premises database is located. They enter the credentials to access the database.



2. They select the database to migrate (`SmartHotel.Registration`).



3. For the target, they enter the name of the managed instance in Azure and the access credentials.



4. In New Activity > Run migration, they specify settings to run the migration:

- Source and target credentials.
- The database to migrate.
- The network share created on the on-premises VM. Azure Database Migration Service takes source backups to this share.
  - The service account that runs the source SQL Server instance must have write permissions on this share.
  - The FQDN path to the share must be used.
- The SAS URI that provides Azure Database Migration Service with access to the storage account container to which the service uploads the backup files for migration.

**Configure migration settings**

Please provide us the SMB network share that Azure Database Migration Service will use to take the source server database backups and SAS URI for the Azure storage container that Azure Database Migration Service will upload those backup files to. Azure Database Migration Service will use these backup files for restore operation.

**Backup settings**

Ensure that the service account running the source SQL Server instance has write privileges on the network location share that you created.

\* Network location share that Azure Database Migration Service can take database backups to

Make sure the Windows user has full control privilege on the network share that you created above. The Azure Database Migration Service will impersonate the user credential to upload the backup files to Azure storage container for restore operation.

\* Windows User Azure Database Migration Service impersonates to upload files to Azure Storage

Password

**Storage account settings**

Provide the SAS URI that allows Azure Database Migration Service to access your storage account container that Azure Database Migration Service will upload the backup files to and use for migrating the databases to SQL DB Managed instance. Use this [link](#) for creating SAS URI, make sure to select all permissions (Read, Write, Delete and List)

\* SAS URI for Azure Storage container that Azure Database Migration Service will upload the files to

5. They save the migration settings and then run the migration.

6. In **Overview**, they monitor the migration status.

The screenshot shows the 'MigrateSmartDB' application interface. At the top, there are four buttons: 'Delete migration', 'Stop migration', 'Refresh' (which is highlighted with a blue border), and 'Download report'. Below these are two sections: 'Source server' and 'Target server'. Under 'Source server', it lists 'sqlvm.contoso.com' and 'Source version SQL Server 2008 R2, 10.50.2500.0'. Under 'Target server', it lists 'contososqlmi.eus25bb65887c364.database.windows.net' and 'Target version Azure SQL Database, 12.0.2000.8'. A section titled 'Server objects' shows a count of 1. Below this is a search bar with placeholder text 'Search to filter items...'. At the bottom, a summary table provides a breakdown of migration status: SERVER OBJECT (Databases), IN PROGRESS (0), STOPPED (0), SUCCESSFUL (1), WARNINGS (0), and FAILED (0).

- When migration is finished, they verify that the target databases exist on the managed instance.

The screenshot shows the Azure portal page for 'contososqlmi' under 'SQL managed instance'. On the left, a sidebar lists navigation options: Overview (selected), Activity log, Tags, Diagnose and solve problems, SETTINGS (Quick start, Connection strings, Active Directory admin, Pricing tier, Locks), and a Feedback button. The main content area displays 'Essentials' settings: Resource group (ContosoRG), Status (Online), Location (East US 2), Subscription name, and Subscription ID. Below this, a summary states '1 managed instance database' with a 'SmartHotel.Registration' link. The 'DATABASE' section shows 'SmartHotel.Registration'.

## Step 7: Migrate the VMs with Azure Migrate: Server Migration

The Contoso admins run a quick test migration and verify the VM is working properly. Then they migrate the VM.

### Run a test migration

- In Migration goals > Servers > Azure Migrate: Server Migration, they select Test migrated servers.

## Migration tools

Azure Migrate: Server Migration

Discover   Replicate   Migrate   Overview

Discovered servers	442
Replicating servers	6
Test migrated servers	1
Migrated servers	1

Next step: You can start migrating the replicating servers to Azure

- They select and hold (or right-click) the VM to test, and then they select **Test migrate**.

Dashboard > Azure Migrate - Servers > Azure Migrate: Server Migration - Replicating machines

Azure Migrate: Server Migration - Replicating machines

Overview   Getting started   Migrate servers to Azure   Manage   Replicating machines   Jobs   Events   Settings   Properties

Name	Status	Health	Migration Phase	Last Sync	Test Migration Status
Contoso-Win2K8R2SP1	Delta sync	Healthy	Test migration pending	2/17/2019, 12:00:43 AM	Never performed

Pin to dashboard   Test migrate   Clean up test migration   Migrate

- In **Test migration**, they select the Azure virtual network in which the Azure VM will be located after the migration. We recommend using a nonproduction virtual network.
- The **Test migration** job starts. They monitor the job in the portal notifications.
- After the migration finishes, they view the migrated Azure VM in **Virtual Machines** in the Azure portal. The machine name has a suffix **-Test**.
- After the test is done, they select and hold (or right-click) the Azure VM in **Replicating machines** and then select **Clean up test migration**.

Refresh   Columns

Last refreshed at: 2/17/2019, 1:02:40 AM

Finished loading data from service.

Filter items...

Name	Status	Health	Migration Phase	Last Sync	Test Migration Status
Contoso-Win2K8R2SP1	Delta sync	Healthy	Test clean up pending	2/17/2019, 12:00:43 AM	2/17/2019, 1:02:40 AM

Pin to dashboard   Test migrate   Clean up test migration   Migrate   Error Details

## Migrate the VM

Now the Contoso admins run a full migration to complete the move.

- In the Azure Migrate project, they go to **Servers > Azure Migrate: Server Migration** and select

## Replicating servers.

The screenshot shows the Azure Migrate: Server Migration interface. At the top, there are four tabs: Discover, Replicate, Migrate, and Overview. The Overview tab is highlighted with a red box. Below the tabs, there are four categories with counts: Discovered servers (58), Replicating servers (1), Test migrated servers (0), and Migrated servers (0). A yellow lightning bolt icon at the bottom left indicates a next step: "Next step: You can start migrating the replicating servers to Azure".

2. In **Replicating machines**, they select and hold (or right-click) the VM, and then they select **Migrate**.
3. In **Migrate > Shut down virtual machines and perform a planned migration with no data loss**, they select **Yes > OK**.
  - By default, Azure Migrate shuts down the on-premises VM and runs an on-demand replication to synchronize any VM changes that occurred since the last replication occurred. This action ensures no data loss.
  - If they don't want to shut down the VM, they select **No**.
4. A migration job starts for the VM. They track the job in Azure notifications.
5. After the job finishes, they can view and manage the VM from the **Virtual Machines** page.
6. Finally, they update the DNS records for **WEBVM** on one of the Contoso domain controllers.

### Update the connection string

As the final step in the migration process, the Contoso admins update the connection string of the application to point to the migrated database that's running on Contoso's SQL managed instance.

1. In the Azure portal, they find the connection string by selecting **Settings > Connection strings**.

The screenshot shows the Azure portal interface for managing a SQL managed instance. On the left, there's a sidebar with navigation links like Overview, Activity log, Tags, Diagnose and solve problems, Quick start, and Connection strings. The Connection strings link is highlighted. At the top, the instance name is shown as contososqlmi - Connection strings. The main content area has tabs for ADO.NET, JDBC, ODBC, and PHP, with ADO.NET being the active tab. It displays a connection string template and a link to download the ADO.NET driver.

2. They update the string with the user name and password of the SQL managed instance.
3. After the string is configured, they replace the current connection string in the `web.config` file of its application.
4. After they update the file and save it, they restart IIS on `WEBVM` by running `iisreset /restart` in a command prompt window.
5. After IIS is restarted, the application uses the database that's running on the SQL managed instance.
6. At this point, they can shut down the on-premises SQLVM machine. The migration is finished.

#### Need more help?

- Learn how to [run a test failover](#).
- Learn how to [create a recovery plan](#).
- Learn how to [fail over to Azure](#).

## Clean up after migration

With the migration finished, the SmartHotel360 application is running on an Azure VM and the SmartHotel360 database is available in the Azure SQL managed instance.

Now, Contoso needs to perform these cleanup tasks:

- Remove the `WEBVM` machine from the vCenter Server inventory.
- Remove the `SQLVM` machine from the vCenter Server inventory.
- Remove `WEBVM` and `SQLVM` from local backup jobs.
- Update internal documentation to show the new location and IP address for `WEBVM`.
- Remove `SQLVM` from internal documentation. Alternatively, Contoso can revise the documentation to show `SQLVM` as deleted and no longer in the VM inventory.
- Review any resources that interact with the decommissioned VMs. Update any relevant settings or documentation to reflect the new configuration.

## Review the deployment

With the migrated resources in Azure, Contoso needs to fully operationalize and secure its new infrastructure.

### Security

The Contoso security team reviews the Azure VMs and SQL managed instance to check for any security issues with its implementation:

- The team reviews the network security groups that are used to control access for the VM. Network security groups help ensure that only traffic that's allowed to the application can pass.
- Contoso's security team also is considering securing the data on the disk by using Azure Disk Encryption and Azure Key Vault.
- The team enables threat detection on the managed instance. Threat detection sends an alert to Contoso's security team/service desk system to open a ticket if a threat is detected. Learn more about [threat detection for SQL Managed Instance](#).

The screenshot shows the Azure portal interface for managing a SQL Managed Instance named "contososqlmi". The left sidebar lists various management options like Overview, Activity log, Tags, and Diagnose and solve problems. The main pane is titled "Threat Detection" and contains a switch labeled "ON" which is highlighted in purple. Below the switch, there are sections for "Storage details" (contosovmadiageus2), "Threat Detection types" (set to "All"), and "Send alerts to" (with the email address "security@contosoc.com" entered). A checked checkbox indicates that alerts will also be sent to "Email service and co-administrators".

To learn more about security practices for VMs, see [Security best practices for IaaS workloads in Azure](#).

### Business continuity and disaster recovery

For business continuity and disaster recovery, Contoso takes the following actions:

- **Keep data safe.** Contoso backs up the data on the VMs by using the Azure Backup service. For more information, see [An overview of Azure VM backup](#).
- **Keep applications up and running.** Contoso replicates the application VMs in Azure to a secondary region using Site Recovery. To learn more, see [Set up disaster recovery to a secondary Azure region for an Azure VM](#).
- **Learn more.** Contoso learns more about managing SQL Managed Instance, which includes [database backups](#).

### Licensing and cost optimization

- Contoso has existing licensing for WEBVM. To take advantage of pricing with Azure Hybrid Benefit, Contoso converts the existing Azure VM.
- Contoso will use [Azure Cost Management and Billing](#) to ensure the company stays within budgets established by the IT leadership.

## Conclusion

In this article, Contoso rehosts the SmartHotel360 application in Azure by migrating the application front-end VM to Azure by using Azure Migrate. Contoso migrates the on-premises database to a SQL managed instance by using Azure Database Migration Service.

# Rehost an on-premises application with Azure VMs and SQL Server Always On availability groups

11/9/2020 • 24 minutes to read • [Edit Online](#)

This article demonstrates how the fictional company Contoso rehosts a two-tier Windows .NET application running on VMware virtual machines (VMs) as part of a migration to Azure. Contoso migrates the application front-end VM to an Azure VM, and the application database to an Azure SQL Server VM, running in a Windows Server failover cluster with SQL Server Always On availability groups.

The SmartHotel360 application used in this example is provided as open source. If you want to use it for your own testing purposes, download it from [GitHub](#).

## Business drivers

The IT leadership team has worked closely with business partners to understand what they want to achieve with this migration. They want to:

- **Address business growth.** Contoso is growing, and as a result there's pressure on on-premises systems and infrastructure.
- **Increase efficiency.** Contoso needs to remove unnecessary procedures and streamline processes for developers and users. The business needs IT to be fast and not waste time or money to deliver faster on customer requirements.
- **Increase agility.** Contoso IT needs to be more responsive to the needs of the business. It must react faster than the changes in the marketplace to enable success in a global economy. IT mustn't get in the way or become a business blocker.
- **Scale.** As the business grows successfully, Contoso IT must provide systems that grow at the same pace.

## Migration goals

The Contoso cloud team has pinned down goals for this migration. These goals were used to determine the best migration method:

- After migration, the application in Azure should have the same performance capabilities as it does today in VMware. The application will remain as critical in the cloud as it is on-premises.
- Contoso doesn't want to invest in this application. It's important to the business, but in its current form, Contoso simply wants to move it safely to the cloud.
- The on-premises database for the application has had availability issues. Contoso want to deploy it in Azure as a high-availability cluster with failover capabilities.
- Contoso wants to upgrade from its current SQL Server 2008 R2 platform to SQL Server 2017.
- Contoso doesn't want to use Azure SQL Database for this application and is looking for alternatives.

## Solution design

After pinning down the company's goals and requirements, Contoso designs and reviews a deployment solution and identifies the migration process. The Azure services that it will use for the migration also are identified.

### Current architecture

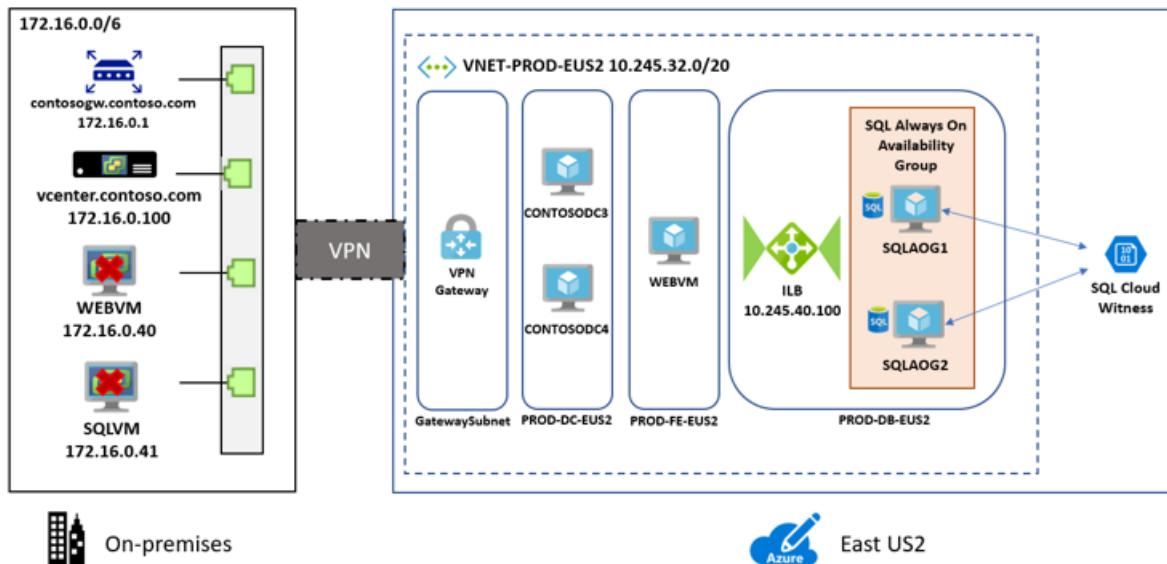
- The application is tiered across two VMs (`WEBVM` and `SQLVM`).
- The VMs are located on VMware ESXi host `contosohost1.contoso.com` (version 6.5).

- The VMware environment is managed by vCenter Server 6.5 (`vcenter.contoso.com`) that runs on a VM.
- Contoso has an on-premises datacenter (`contoso-datacenter`) with an on-premises domain controller (`contosodc1`).

## Proposed architecture

In this scenario:

- Contoso will migrate the application front end `WEBVM` to an Azure infrastructure as a service (IaaS) VM.
  - The front-end VM in Azure will be deployed in the `ContosoRG` resource group (used for production resources).
  - It will be located in the Azure production network (`VNET-PROD-EU2`) in the primary region (`East US 2`).
- The application database will be migrated to an Azure SQL Server VM.
  - It will be located in Contoso's Azure database network (`PROD-DB-EU2`) in the primary region (`East US 2`).
  - It will be placed in a Windows Server failover cluster with two nodes that uses SQL Server Always On availability groups.
    - In Azure, the two SQL Server VM nodes in the cluster will be deployed in the `ContosoRG` resource group.
    - The VM nodes will be located in the Azure production network (`VNET-PROD-EU2`) in the primary region (`East US 2`).
    - VMs will run Windows Server 2016 with SQL Server 2017 Enterprise edition. Contoso doesn't have licenses for this operating system. It will use an image in Azure Marketplace that provides the license as a charge to the company's Azure Enterprise Agreement commitment.
    - Apart from unique names, both VMs use the same settings.
- Contoso will deploy an internal load balancer that listens for traffic on the cluster and directs it to the appropriate cluster node.
  - The internal load balancer will be deployed in `ContosoNetworkingRG` (used for networking resources).
- The on-premises VMs in the Contoso datacenter will be decommissioned after the migration is done.



## Database considerations

As part of the solution design process, Contoso did a feature comparison between Azure SQL Database and SQL Server. The following considerations helped the company to decide to use an Azure IaaS VM running SQL Server:

- Using an Azure VM running SQL Server seems to be an optimal solution if Contoso needs to customize the operating system or the database server, or if it might want to colocate and run third-party applications on the same VM.

## Solution review

Contoso evaluates its proposed design by putting together a list of pros and cons.

CONSIDERATION	DETAILS
Pros	<p><b>WEBVM</b> will be moved to Azure without changes, which makes the migration simple.</p> <p>The SQL Server tier will run on SQL Server 2017 and Windows Server 2016, which retires the current Windows Server 2008 R2 operating system. Running SQL Server 2017 supports Contoso's technical requirements and goals. It provides 100 percent compatibility while moving away from SQL Server 2008 R2.</p> <p>Contoso can take advantage of its investment in Software Assurance by using the Azure Hybrid Benefit.</p> <p>A high-availability SQL Server deployment in Azure provides fault tolerance so that the application data tier is no longer a single point of failover.</p>
Cons	<p><b>WEBVM</b> is running Windows Server 2008 R2. The operating system is supported by Azure for specific roles (July 2018). To learn more, see <a href="#">Microsoft server software support for Microsoft Azure virtual machines</a>.</p> <p>The web tier of the application remains a single point of failover.</p> <p>Contoso needs to continue supporting the web tier as an Azure VM rather than moving to a managed service such as Azure App Service.</p> <p>With the chosen solution, Contoso will need to continue managing two SQL Server VMs rather than moving to a managed platform, such as Azure SQL Managed Instance. In addition, with Software Assurance, Contoso could exchange its existing licenses for discounted rates on Azure SQL Managed Instance.</p>

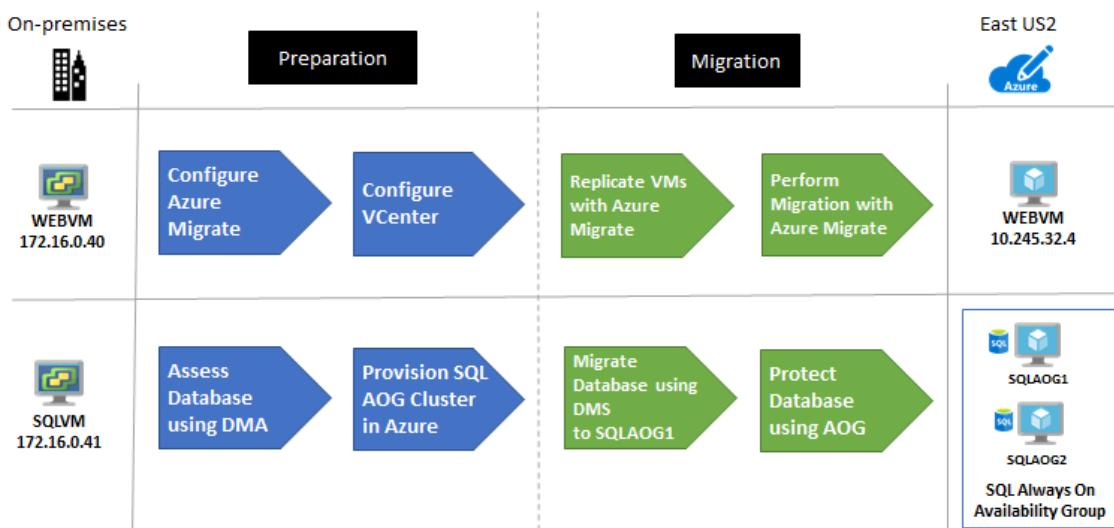
## Azure services

SERVICE	DESCRIPTION	COST
<a href="#">Azure Database Migration Service</a>	Azure Database Migration Service enables seamless migration from multiple database sources to Azure data platforms with minimal downtime.	Learn about <a href="#">supported regions</a> and <a href="#">Azure Database Migration Service pricing</a> .
<a href="#">Azure Migrate</a>	Contoso uses Azure Migrate to assess its VMware VMs. Azure Migrate assesses the migration suitability of the machines. It provides sizing and cost estimates for running in Azure.	Azure Migrate is available at no additional charge. They might incur charges depending on the tools (first-party or independent software vendor) they decide to use for assessment and migration. Learn more about <a href="#">Azure Migrate pricing</a> .

## Migration process

The Contoso admins will migrate the application VMs to Azure.

- They'll migrate the front-end VM to Azure VM by using Azure Migrate:
  - As a first step, they'll prepare and set up Azure components and prepare the on-premises VMware infrastructure.
  - With everything prepared, they can start replicating the VM.
  - After replication is enabled and working, they migrate the VM by using Azure Migrate.
- After they've verified the database, they'll migrate the database to a SQL Server cluster in Azure by using Azure Database Migration Service.
  - As a first step, they'll need to provision SQL Server VMs in Azure, set up the cluster and an internal load balancer, and configure Always On availability groups.
  - With this in place, they can migrate the database.
- After the migration, they'll enable Always On availability groups for the database.



## Prerequisites

Here's what Contoso needs to do for this scenario.

REQUIREMENTS	DETAILS
Azure subscription	<p>Contoso already created a subscription in an earlier article in this series. If you don't have an Azure subscription, create a <a href="#">free account</a>.</p> <p>If you create a free account, you're the administrator of your subscription and can perform all actions.</p> <p>If you use an existing subscription and you're not the administrator, work with the admin to assign you Owner or Contributor permissions.</p>

Requirements	Details
Azure infrastructure	Contoso set up the Azure infrastructure as described in <a href="#">Azure infrastructure for migration</a> .  Learn more about specific <a href="#">prerequisites</a> requirements for Azure Migrate: Server Migration.
On-premises servers	The on-premises vCenter Server should be running version 5.5, 6.0, 6.5, or 6.7.  An ESXi host running version 5.5, 6.0, 6.5, or 6.7.  One or more VMware VMs running on the ESXi host.
On-premises VMs	<a href="#">Review Linux machines</a> that are endorsed to run on Azure.

## Scenario steps

Here's how Contoso will run the migration:

- **Step 1: Prepare a SQL Server Always On availability group cluster.** Create a cluster for deploying two SQL Server VM nodes in Azure.
- **Step 2: Deploy and set up the cluster.** Prepare an Azure SQL Server cluster. Databases are migrated into this existing cluster.
- **Step 3: Deploy Azure Load Balancer.** Deploy a load balancer to balance traffic to the SQL Server nodes.
- **Step 4: Prepare Azure for Azure Migrate.** Create an Azure Storage account to hold replicated data.
- **Step 5: Prepare on-premises VMware for Azure Migrate.** Prepare accounts for VM discovery and agent installation. Prepare on-premises VMs so that users can connect to Azure VMs after migration.
- **Step 6: Replicate the on-premises VMs to Azure.** Enable VM replication to Azure.
- **Step 7: Migrate the database via Azure Database Migration Service.** Migrate the database to Azure by using Azure Database Migration Service.
- **Step 8: Protect the database with SQL Server Always On.** Create an Always On availability group for the cluster.
- **Step 9: Migrate the VM with Azure Migrate.** Run a test migration to make sure everything's working as expected. Then run a migration to Azure.

## Step 1: Prepare a SQL Server Always On availability group cluster

To set up the cluster, the Contoso admins:

1. Create two SQL Server VMs by selecting SQL Server 2017 Enterprise Windows Server 2016 image in the Azure Marketplace.



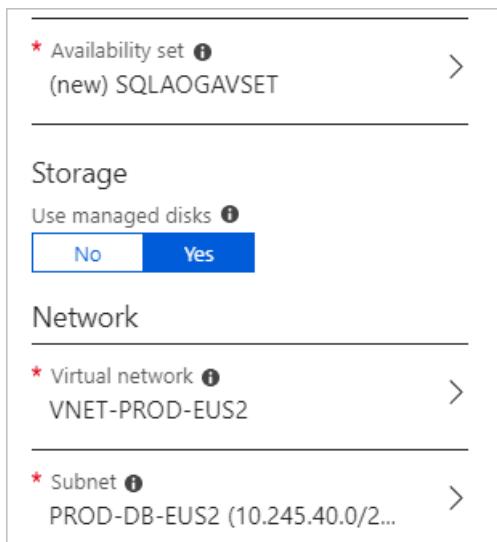
2. In **Create Virtual Machine Wizard > Basics**, they configure:

- Names for the VMs: `SQLAOG1` and `SQLAOG2`.
- Because machines are business-critical, enable SSD for the VM disk type.
- Specify machine credentials.
- They deploy the VMs in the primary region (`East US 2`) in the `ContosoRG` resource group.

3. In **Size**, they start with **D2S v3** instances for both VMs. They'll scale later as needed.

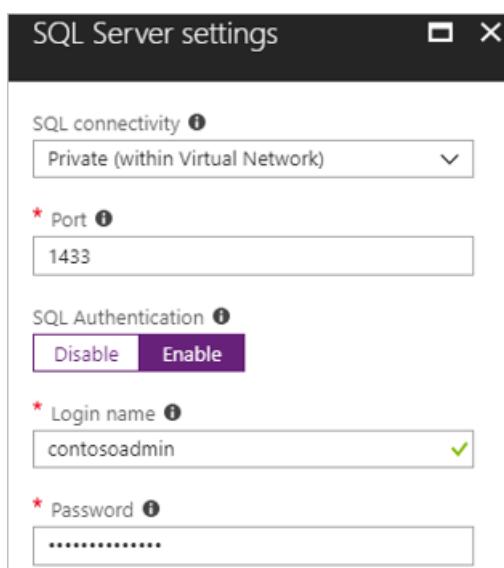
4. In **Settings**, they do the following actions:

- Because these VMs are critical databases for the application, they use managed disks.
- They place the machines in the database subnet (**PROD-DB-EUS2**) of the production network (**VNET-PROD-EUS2**) in the primary region (**East US 2**).
- They create a new availability set (**SQLAOGAVSET**) with two fault domains and five update domains.



5. In **SQL Server settings**, they limit SQL connectivity to the virtual network (private) on default port 1433.

For authentication, they use the same credentials as used on-site (**contosoadmin**).



#### Need more help?

- Get help with how to [provision a SQL Server VM](#).
- Learn about how to [configure VMs for different SQL Server SKUs](#).

## Step 2: Deploy and set up the cluster

To set up the cluster, the Contoso admins:

- Set up an Azure Storage account to act as the cloud witness.
- Add the SQL Server VMs to the Active Directory domain in the Contoso on-premises datacenter.
- Create the cluster in Azure.

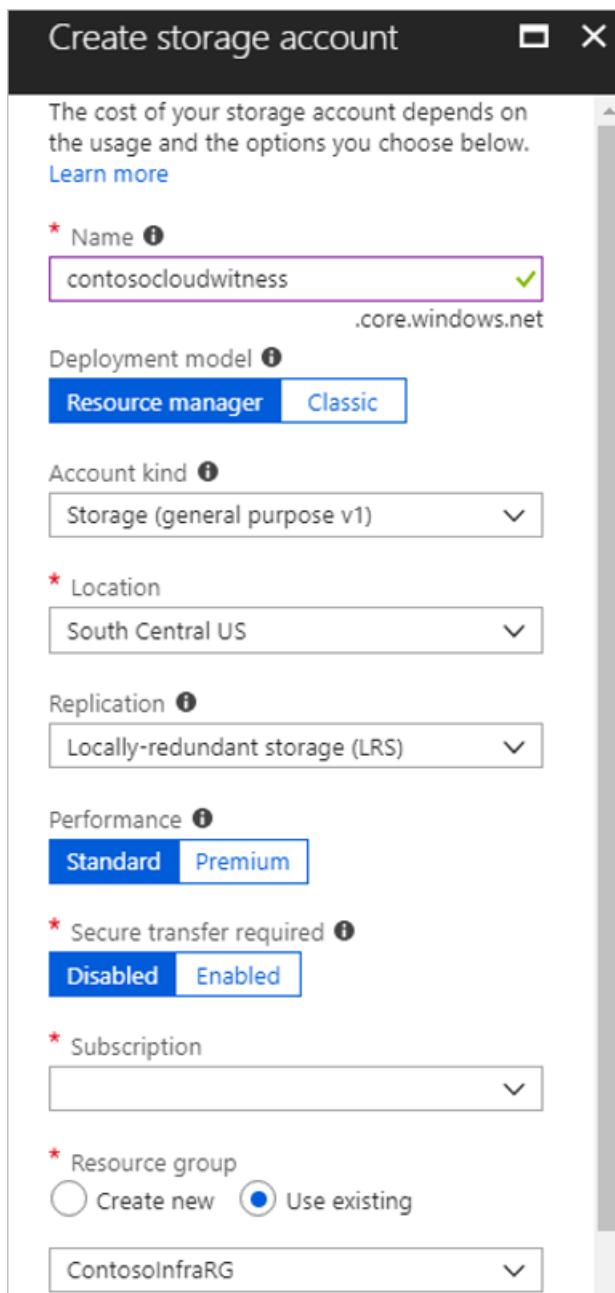
4. Configure the cloud witness.
5. Enable SQL Always On availability groups.

### Set up a storage account as a cloud witness

To set up a cloud witness, Contoso needs an Azure Storage account that will hold the blob file used for cluster arbitration. The same storage account can be used to set up cloud witness for multiple clusters.

To create a storage account, the Contoso admins:

1. Specify a recognizable name for the account (`contosocloudwitness`).
2. Deploy a general all-purpose account, with LRS.
3. Place the account in a third region (`South Central US`). They place it outside the primary and secondary region so that it remains available during regional failure.
4. Place it in the resource group that holds infrastructure resources, `ContosoInfraRG`.



5. When they create the storage account, primary and secondary access keys are generated for it. They need the primary access key to create the cloud witness. The key appears under the storage account name > **Access keys**.

Storage account name

contosocloudwitness

key1 

Key

/osRx/v7uLlc0uXSj7jzYsCMBJtHDKLKSpf15rrxuZ

#### Add SQL Server VMs to Contoso domain

1. Contoso adds `SQLAOG1` and `SQLAOG2` to the `contoso.com` domain.
2. On each VM, the admins install the Windows Failover Cluster feature and tools.

#### Set up the cluster

Before the Contoso admins set up the cluster, they take a snapshot of the OS disk on each machine.

Create snapshot

\* Name  
SQLAOG1-Before-Cluster 

\* Subscription

\* Resource group  
 Create new  Use existing  
ContosoRG 

\* Location  
East US 2 

\* Account type   
Standard (HDD) 

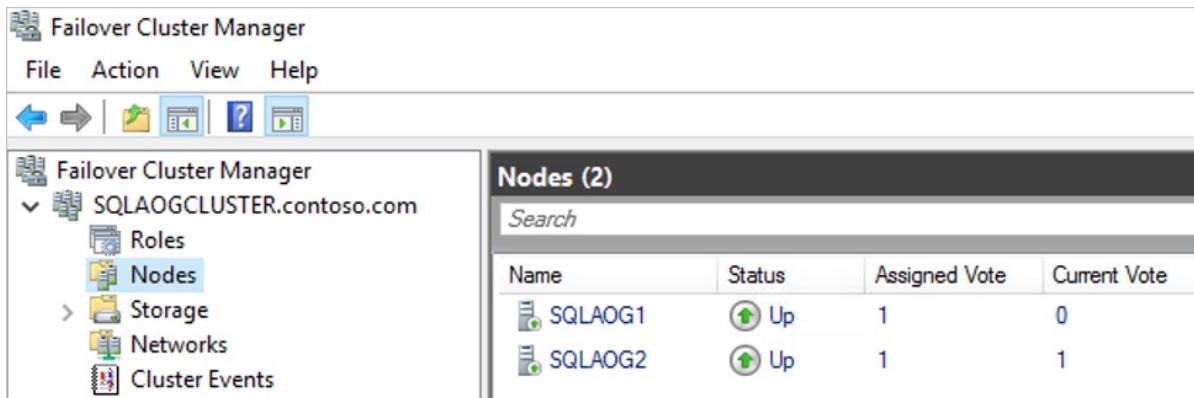
1. They run a script to create the Windows failover cluster.

```

ClusterCreateSQLAOG.ps1 X
1 <#
2 Microsoft Cloud Workshop: BCDR
3 .File Name
4 - ClusterCreateSQLAOG.ps1
5
6 .What calls this script?
7 - This is run manually on SQLAOG1 to create the Windows Failover Cluster
8
9 .What does this script do?
10 - The Result will be a Cluster Named AOGCLUSTER running on the 10.245.40.99 IP Address
11   with the hostname of SQLAOGCLUSTER.CONTOSO.COM
12
13 - Two Cluster Networks will be created Cluster Network 1 (10.245.40.0/24)
14 #>
15 New-Cluster -Name SQLAOGCLUSTER -Node SQLAOG1,SQLAOG2 -StaticAddress 10.245.40.99
16

```

- After the cluster is created, they verify that the VMs appear as cluster nodes.



### Configure the cloud witness

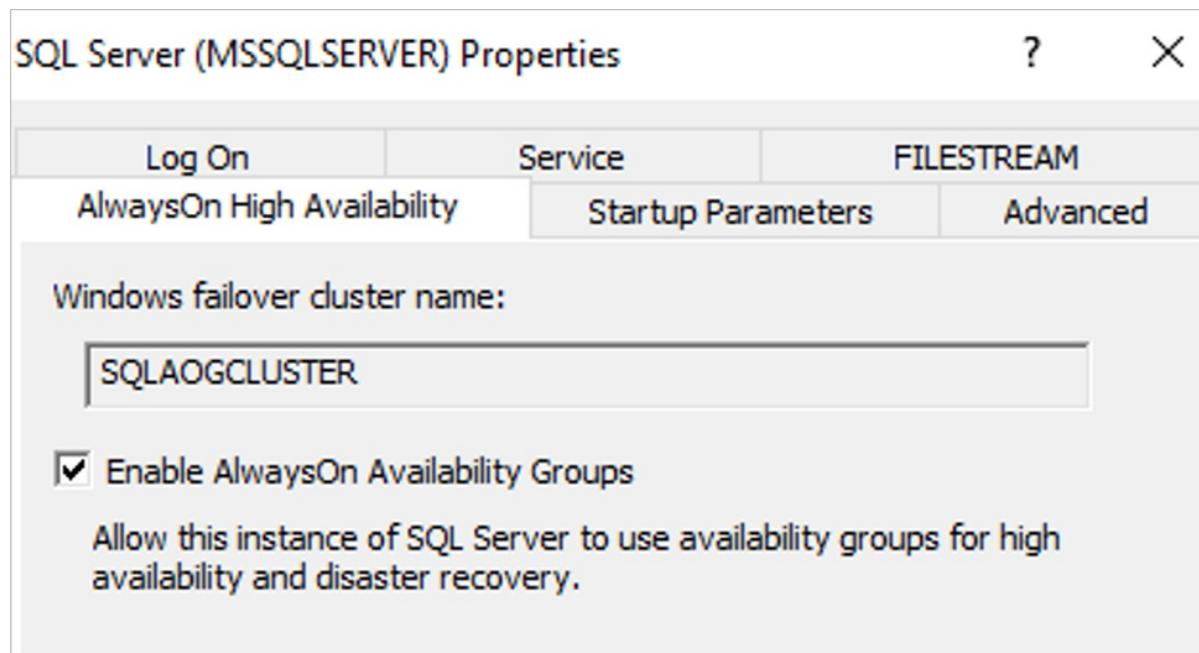
- The Contoso admins configure the cloud witness by using the Quorum Configuration Wizard in Failover Cluster Manager.
- In the wizard, they select to create a cloud witness with the storage account.
- After the cloud witness is configured, it appears in the Failover Cluster Manager snap-in.



### Enable SQL Server Always On availability groups

The Contoso admins can now enable Always On availability groups:

- In SQL Server Configuration Manager, they enable Always On availability groups for the SQL Server (MSSQLSERVER) service.



2. They restart the service for changes to take effect.

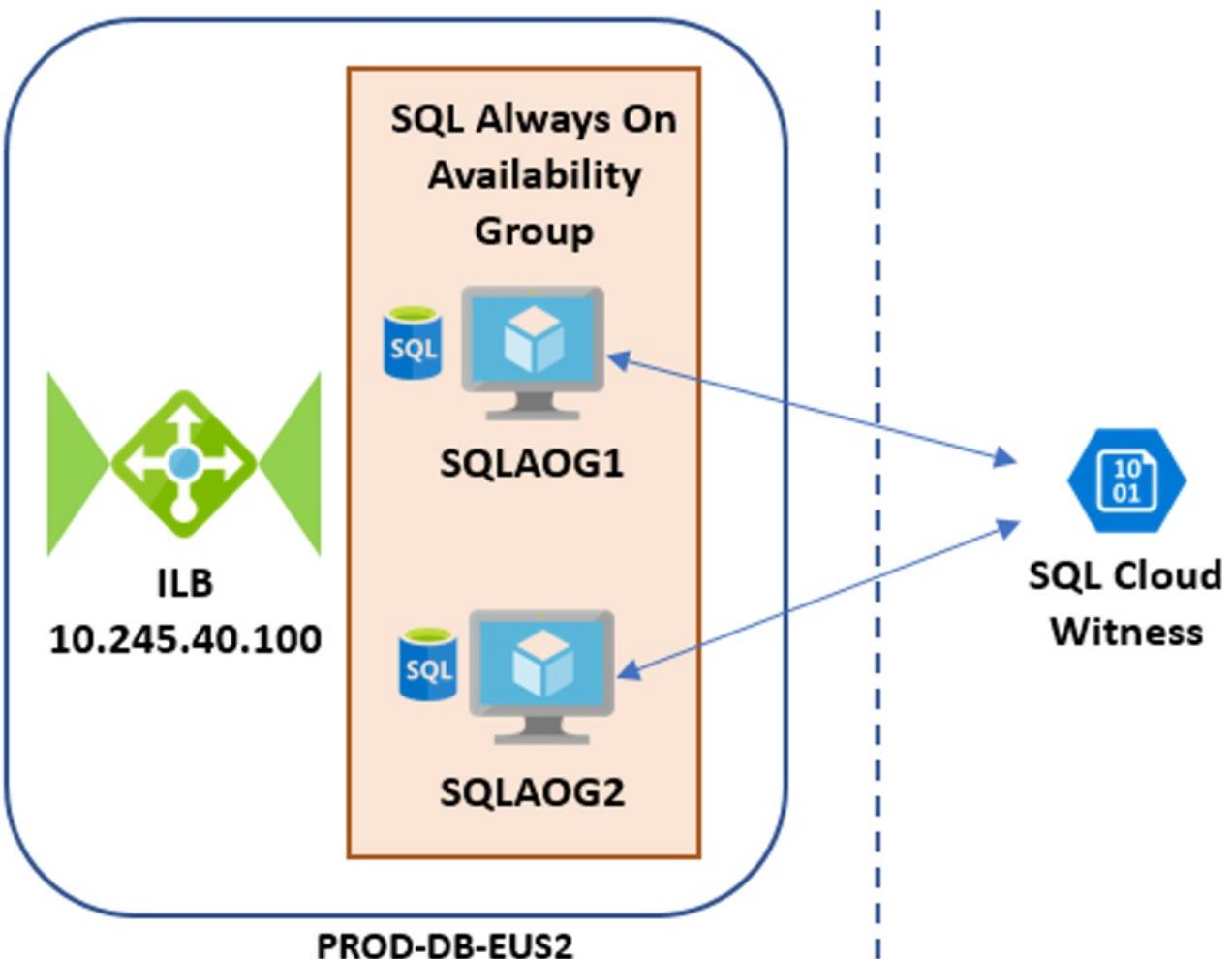
With Always On availability groups enabled, Contoso can set up the Always On availability group that will protect the SmartHotel360 database.

#### Need more help?

- Read about [cloud witness and setting up a storage account for it](#).
- Get instructions for how to [set up a cluster and create an availability group](#).

## Step 3: Deploy Azure Load Balancer

The Contoso admins now want to deploy an internal load balancer that sits in front of the cluster nodes. The load balancer listens for traffic and directs it to the appropriate node.



To create the load balancer, the Contoso admins:

1. In the Azure portal, go to **Networking > Load balancer**, and set up a new internal load balancer: **ILB-PROD-DB-EUS2-SQLAOG**.
2. Place the load balancer in the database subnet (**PROD-DB-EUS2**) of the production network (**VNET-PROD-EUS2**).
3. Assign it a static IP address (**10.245.40.100**).
4. As a networking element, deploy the load balancer in the networking resource group **ContosoNetworkingRG**.

**Create load balancer**

★ Name  
ILB-PROD-DB-EUS2-SQLAOG ✓

★ Type ⓘ  
 Internal  Public

★ SKU ⓘ  
 Basic  Standard

★ Virtual network >  
VNET-PROD-EUS2

★ Subnet >  
PROD-DB-EUS2 (10.245.40.0/2...

★ IP address assignment  
 Static  Dynamic

★ Private IP address  
10.245.40.100 ✓

★ Subscription  
<subscription id> ▾

★ Resource group  
 Create new  Use existing

ContosoNetworkingRG ▾

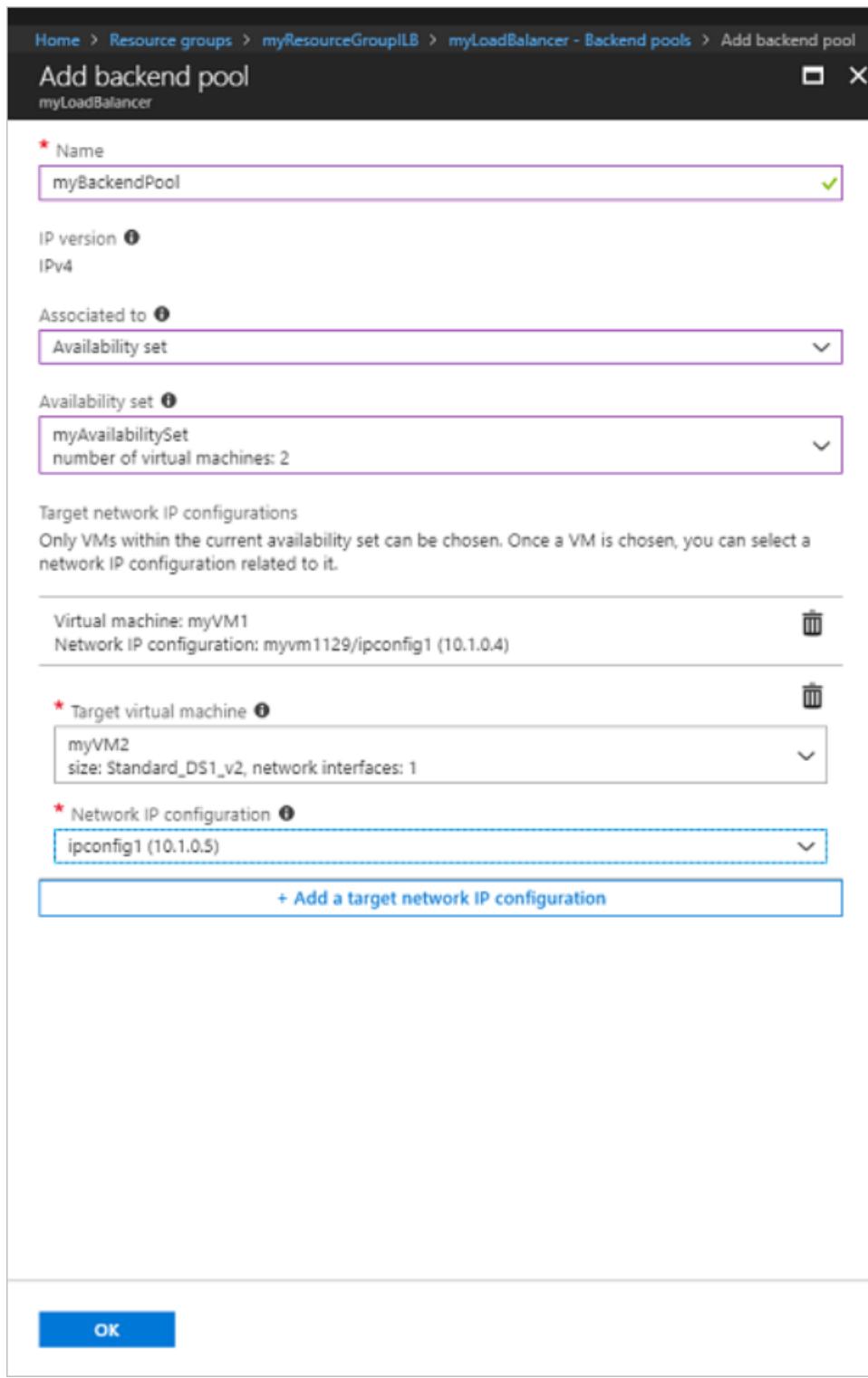
★ Location  
East US 2 ▾

After the internal load balancer is deployed, the Contoso admins need to set it up. They create a back-end address pool, set up a health probe, and configure a load-balancing rule.

### Add a back-end pool

To distribute traffic to the VMs in the cluster, the Contoso admins set up a back-end address pool that contains the IP addresses of the NICs for VMs that will receive network traffic from the load balancer.

1. In the load balancer settings in the portal, Contoso adds a back-end pool: ILB-PROD-DB-EUS-SQLAOG-BEPOOL .
2. The admins associate the pool with availability set SQLAOGAVSET . The VMs in the set ( SQLAOG1 and SQLAOG2 ) are added to the pool.



### Create a health probe

The Contoso admins create a health probe so that the load balancer can monitor the application health. The probe dynamically adds or removes VMs from the load balancer rotation based on how they respond to health checks.

To create the probe, the Contoso admins:

1. In the load balancer settings in the portal, create a health probe: **SQLAlwaysOnEndPointProbe**.
2. Set the probe to monitor VMs on TCP port 59999.
3. Set an interval of 5 seconds between probes and a threshold of 2. If two probes fail, the VM will be considered unhealthy.

Add health probe  
ILB-PROD-DB-EUS2-SQLAOG

\* Name  
SQLAlwaysOnEndPointProbe ✓

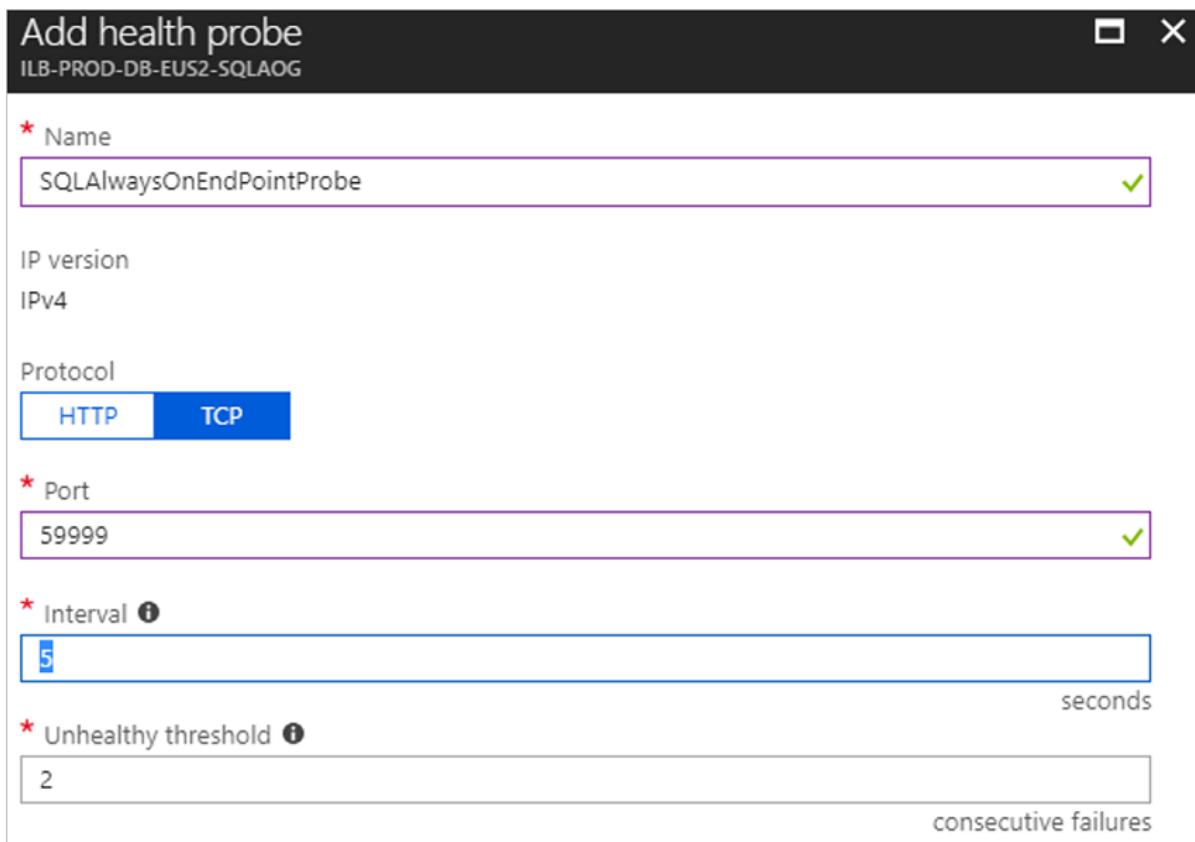
IP version  
IPv4

Protocol  
HTTP TCP

\* Port  
59999 ✓

\* Interval ⓘ  
5 seconds

\* Unhealthy threshold ⓘ  
2 consecutive failures



### Configure the load balancer to receive traffic

Now, the Contoso admins set up a load balancer rule to define how traffic is distributed to the VMs.

- The front-end IP address handles incoming traffic.
- The back-end IP pool receives the traffic.

To create the rule, the Contoso admins:

1. In the load balancer settings in the portal, add a new rule: `SQLAlwaysOnEndPointListener`.
2. Set a front-end listener to receive incoming SQL client traffic on TCP port 1433.
3. Specify the back-end pool to which traffic will be routed and the port on which VMs listen for traffic.
4. Enable floating IP (direct server return), which is always required for SQL Server Always On.

Add health probe  
ILB-PROD-DB-EUS2-SQLAOG

\* Name  
SQLAlwaysOnEndPointProbe ✓

IP version  
IPv4

Protocol  
**HTTP** TCP

\* Port  
59999 ✓

\* Interval ⓘ  
5 seconds

\* Unhealthy threshold ⓘ  
2 consecutive failures

#### Need more help?

- Get an overview of [Azure Load Balancer](#).
- Learn about how to [create a load balancer](#).

## Step 4: Prepare Azure for Azure Migrate

Here are the Azure components Contoso needs to deploy Azure Migrate:

- A virtual network in which VMs will be located when they're migrated.
- An Azure Storage account to hold replicated data.

The Contoso admins set up these components:

1. Contoso already created a network/subnet it can use for Azure Migrate when it [deployed the Azure infrastructure](#).
  - The SmartHotel360 application is a production application, and **WEBVM** will be migrated to the Azure production network (**VNET-PROD-EUS2**) in the primary region (**East US 2**).
  - **WEBVM** will be placed in the **ContosoORG** resource group, which is used for production resources, and in the production subnet (**PROD-FE-EUS2**).
2. The Contoso admins create an Azure Storage account (**contosovmsacc20180528**) in the primary region.
  - Use a general-purpose account with standard storage and LRS replication.

## Step 5: Prepare on-premises VMware for Azure Migrate

Here's what the Contoso admins prepare on-premises:

- An account on the vCenter Server or vSphere ESXi host to automate VM discovery.
- On-premises VM settings so that Contoso can connect to the replicated Azure VM after migration.

#### Prepare an account for automatic discovery

Azure Migrate needs access to VMware servers to:

- Automatically discover VMs.
- Orchestrate replication and migration.
- At least a read-only account is required. They need an account that can run operations such as creating and removing disks and turning on VMs.

To set up the account, the Contoso admins:

1. Create a role at the vCenter level.
2. Assign that role the required permissions.

### Prepare to connect to Azure VMs after migration

After migration, Contoso wants to connect to the Azure VMs and allow Azure to manage the VMs. To do this, the Contoso admins do the following tasks before migration:

1. For access over the internet, they:
  - Enable RDP or SSH on the on-premises VM before migration.
  - Ensure that TCP and UDP rules are added for the **Public** profile.
  - Check that RDP or SSH is allowed in the operating system firewall.
2. For access over site-to-site VPN, they:
  - Enable RDP or SSH on the on-premises VM before migration.
  - Check that RDP or SSH is allowed in the operating system firewall.
  - For Windows, set the operating system's SAN policy on the on-premises VM to **OnlineAll**.
3. Install the Azure agent:
  - [Azure Linux agent](#)
  - [Azure Windows agent](#)
4. Miscellaneous
  - For Windows, there should be no Windows updates pending on the VM when triggering a migration. If there are, the Contoso admins won't be able to sign in to the VM until the update completes.
  - After migration, they can check **Boot diagnostics** to view a screenshot of the VM. If it doesn't work, they should verify that the VM is running and review these [troubleshooting tips](#).

### Need more help?

Learn about how to [prepare VMs for migration](#).

## Step 6: Replicate the on-premises VMs to Azure

Before the Contoso admins can run a migration to Azure, they need to set up and enable replication.

With discovery finished, they can begin replication of VMware VMs to Azure.

1. In the Azure Migrate project, they go to **Servers > Azure Migrate: Server Migration**, and select **Replicate**.

The screenshot shows the Azure Migrate - Servers dashboard. On the left, there's a sidebar with navigation links: Overview, Migration goals, Servers (which is selected), Databases, Data Box, Manage, Discovered items, Support + troubleshooting, and New support request. The main content area has a header "Assessment tools". It features a box titled "Azure Migrate: Server Assessment" with tabs Discover, Assess, and Overview. Under Discover, it shows 442 Discovered servers, 2 Groups, 2 Assessments, and 0 Notifications. A callout says "Next step: Start migrating your servers or optionally you can refine your application grouping with dependency analysis". Below this is a link "Add more assessment tools? Click here." Another box titled "Migration tools" contains a "Azure Migrate: Server Migration" section with tabs Discover, Replicate (which is highlighted with a red box), Migrate, and Overview. It shows 442 Discovered servers.

2. In Replicate > Source settings > Are your machines virtualized?, they select Yes, with VMware vSphere.
3. In On-premises appliance, they select the name of the Azure Migrate appliance that was set up, and then select OK.

The screenshot shows the "Replicate" configuration page. At the top, there are tabs: Source settings (which is selected and underlined), Virtual machines, Target settings, Compute, Disks, and Review + Start replication. Below the tabs, a note says "The first step in migrating servers is to replicate them. Once replication completes, you can perform test migration before finally moving the servers to Azure." There are two required fields: "Are your machines virtualized?" with the value "Yes, with VMware vSphere" and "On-premises appliance" with the value "<appliance-name>".

4. In Virtual machines, they select the machines to replicate.
  - If the Contoso admins have run an assessment for the VMs, they can apply VM sizing and disk type (premium/standard) recommendations from the assessment results. In Import migration settings from an Azure Migrate assessment?, they select the Yes option.

- If they didn't run an assessment or don't want to use the assessment settings, they select the **No** option.
- If they selected to use the assessment, they select the VM group and assessment name.

**Replicate**

Source settings   **Virtual machines**   Target settings   Compute   Disks   Review + Start replication

Select the virtual machines to be migrated.

\* Import migration settings from an assessment? (i)

**Select**

Yes, apply migration settings from a Azure Migrate assessment  
No, I'll specify the migration settings manually

5. In **Virtual machines**, they search for VMs as needed and check each VM to migrate. Then they select **Next: Target settings**.
6. In **Target settings**, they select the subscription, and target region to which they'll migrate, and specify the resource group in which the Azure VMs will reside after migration. In **Virtual Network**, they select the Azure virtual network/subnet to which the Azure VMs will be joined after migration.
7. In **Azure Hybrid Benefit**, the Contoso admins:
  - Select **No** if they don't want to apply Azure Hybrid Benefit. Then they select **Next**.
  - Select **Yes** if they have Windows Server machines that are covered with active Software Assurance or Windows Server subscriptions, and they want to apply the benefit to the machines they're migrating. Then they select **Next**.
8. In **Compute**, they review the VM name, size, OS disk type, and availability set. VMs must conform with [Azure requirements](#).
  - **VM size:** If they're using assessment recommendations, the VM size drop-down list contains the recommended size. Otherwise, Azure Migrate picks a size based on the closest match in the Azure subscription. Alternatively, they can pick a manual size in **Azure VM size**.
  - **OS disk:** They specify the OS (boot) disk for the VM. The OS disk is the disk that has the operating system bootloader and installer.
  - **Availability set:** If the VM should be in an Azure availability set after migration, they specify the set. The set must be in the target resource group specified for the migration.
9. In **Disks**, they specify whether the VM disks should be replicated to Azure. Then they select the disk type (standard SSD/HDD or premium managed disks) in Azure and select **Next**.
  - They can exclude disks from replication.
  - If disks are excluded, they won't be present on the Azure VM after migration.
10. In **Review + Start replication**, they review the settings. Then they select **Replicate** to start the initial replication for the servers.

**NOTE**

Replication settings can be updated any time before replication starts in **Manage > Replicating machines**. Settings can't be changed after replication starts.

## Step 7: Migrate the database via Azure Database Migration Service

The Contoso admins migrate the database via Azure Database Migration Service by following the [step-by-step](#)

migration tutorial. They can perform online, offline, and hybrid (preview) migrations.

As a summary, they must perform the following tasks:

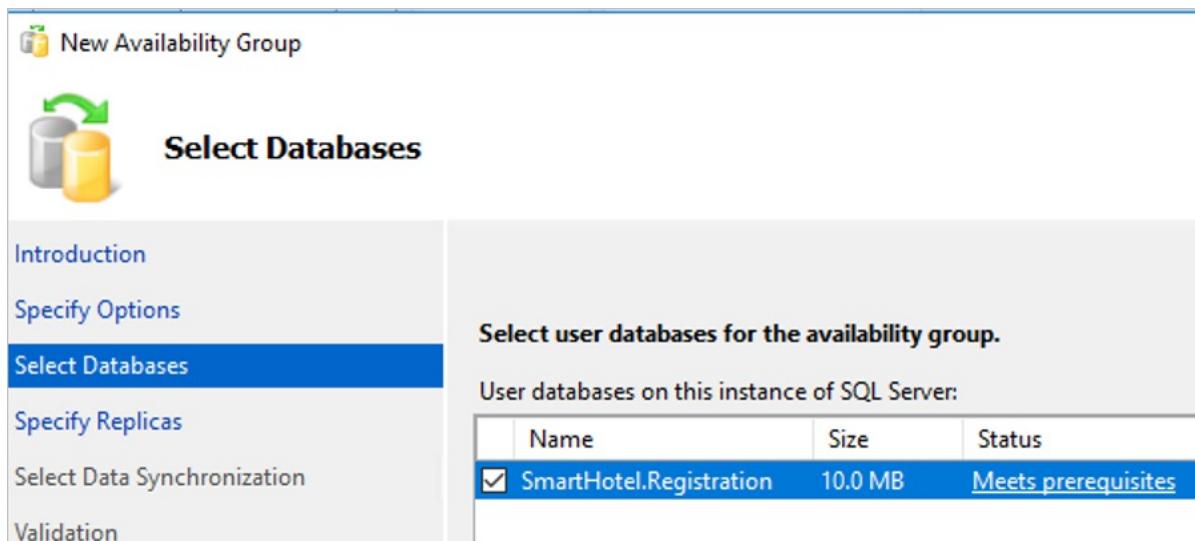
- Use the Premium pricing tier to create an Azure Database Migration Service instance that connects to the virtual network.
- Ensure that the instance can access the remote SQL Server via the virtual network. Ensure that all incoming ports are allowed from Azure to SQL Server at the virtual network level, the network VPN, and the machine that hosts SQL Server.
- Configure the instance:
  - Create a migration project.
  - Add a source (on-premises database).
  - Select a target.
  - Select the databases to migrate.
  - Configure advanced settings.
  - Start the replication.
  - Resolve any errors.
  - Perform the final cutover.

## Step 8: Protect the database with SQL Server Always On

With the application database running on `SQLAOG1`, the Contoso admins can now protect it by using Always On availability groups. They configure SQL Server Always On by using SQL Server Management Studio and then assign a listener by using Windows clustering.

### Create an Always On availability group

1. In SQL Server Management Studio, they select and hold (or right-click) **Always On High Availability** to start the **New Availability Group Wizard**.
2. In **Specify Options**, they name the availability group `SHAOG`. In **Select Databases**, they select the `SmartHotel1360` database.



3. In **Specify Replicas**, they add the two SQL nodes as availability replicas and configure them to provide automatic failover with synchronous commit.

## Specify an instance of SQL Server to host a secondary replica.

Replicas Endpoints Backup Preferences Listener Read-Only Routing

Availability Replicas:

Server Instance	Initial Role	Automatic Failover (Up to 3)	Availability Mode
SQLAOG1	Primary	<input checked="" type="checkbox"/>	Synchronous commit
SQLAOG2	Secondary	<input checked="" type="checkbox"/>	Synchronous commit

4. They configure a listener for the group ( SHAOG ) and port. The IP address of the internal load balancer is added as a static IP address ( 10.245.40.100 ).

Specify an instance of SQL Server to host a secondary replica.

Replicas Endpoints Backup Preferences Listener Read-Only Routing

Specify your preference for an availability group listener that will provide a cl

Do not create an availability group listener now  
You can create the listener later using the Add Availability Group Listener

Create an availability group listener  
Specify your listener preferences for this availability group.

Listener DNS Name:	SHAOG
Port:	1433
Network Mode:	Static IP
Subnet	IP Address
10.245.40.0/23	10.245.40.100

5. In Select Data Synchronization, they enable automatic seeding. With this option, SQL Server automatically creates secondary replicas for every database in the group, so Contoso doesn't have to manually back up and restore them. After validation, the availability group is created.

The wizard completed successfully.

Summary:

Name	Result
Configuring endpoints.	Success
Starting the 'AlwaysOn_health' extended events session on 'SQLAOG1'.	Success
Configuring endpoints.	Success
Starting the 'AlwaysOn_health' extended events session on 'SQLAOG2'.	Success
Creating availability group 'SHAOG'.	Success
Waiting for availability group 'SHAOG' to come online.	Success
Creating Availability Group Listener 'SHAOG'.	Success
Joining secondaries to availability group 'SHAOG'.	Success
Validating Windows Failover Cluster quorum vote configuration.	Success

6. Contoso ran into an issue when creating the group. It isn't using Active Directory Windows integrated security and needs to grant permissions to the SQL login to create the Windows failover cluster roles.

```

GRANT ALTER ANY AVAILABILITY GROUP TO [NT AUTHORITY\SYSTEM];
GRANT CONNECT SQL TO [NT AUTHORITY\SYSTEM];
GRANT VIEW SERVER STATE TO [NT AUTHORITY\SYSTEM];

```

7. After the group is created, it appears in SQL Server Management Studio.

### Configure a listener on the cluster

As a last step in setting up the SQL deployment, the Contoso admins configure the internal load balancer as the listener on the cluster and bring the listener online. They use a script to do this task.

```

<#
Contoso Cloud Migration
.File Name
- ClusterUpdateSQLAOG.ps1

.What calls this script?
- Run this script on SQLAOG1 to update Windows Failover Cluster, but only after
  ClusterCreateSQLAOG.ps1 has been successfully executed and the steps to establish
  the SQL Always On Availability Group have been completed.

.What does this script do?
- This script creates the Windows Failover Client IP probes that are required to determine
  which nodes are online.

#>

$ClusterNetworkName = "Cluster Network 1"
$IPResourceName = "SHAOG_10.245.40.100"
$ILBIP = "10.245.40.100"
Import-Module FailoverClusters
Get-ClusterResource $IPResourceName | Set-ClusterParameter -Multiple @{"Address"="$ILBIP"; "Pr
Stop-ClusterResource -Name $IPResourceName
Start-ClusterResource -Name "SHAOG"

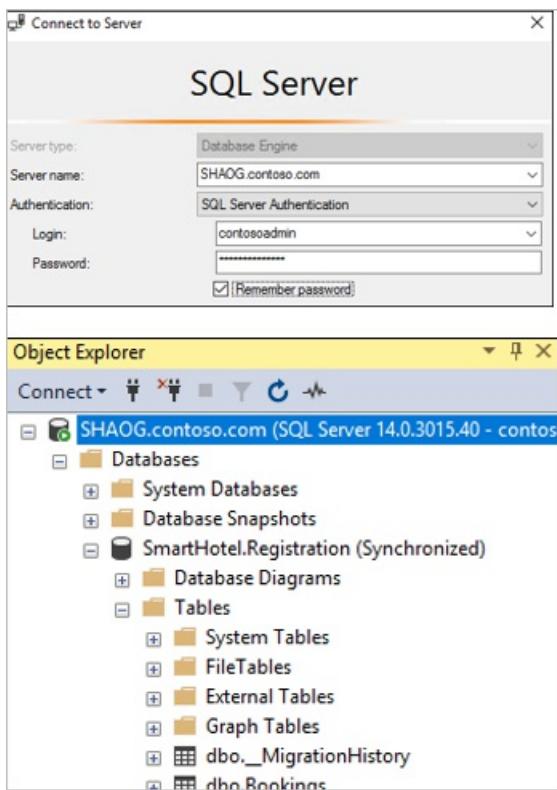
```

PS C:\Users\administrator\Desktop> C:\Users\administrator\Desktop\ClusterUpdateSQLAOG.ps1  
WARNING: The properties were stored, but not all changes will take effect until SHAOG\_10.245.40.100

Name	State	OwnerGroup	ResourceType
SHAOG_10.245.40.100	Offline	SHAOG	IP Address
SHAOG	Online	SHAOG	SQL Server Availability Group

### Verify the configuration

With everything set up, Contoso now has a functional availability group in Azure that uses the migrated database. The admins verify the configuration by connecting to the internal load balancer in SQL Server Management Studio.



#### Need more help?

- Learn about how to create an [availability group](#) and [listener](#).
- Manually [set up the cluster to use the load balancer IP address](#).
- Learn more about how to [create and use SAS](#).

## Step 9: Migrate the VM with Azure Migrate

The Contoso admins run a quick test failover and then migrate the VM.

### Run a test migration

Running a test migration helps ensure that everything's working as expected before the migration. The Contoso admins:

1. Run a test failover to the latest available point in time (`Latest processed`).
2. Select **Shut down machine before beginning failover** so that Azure Migrate attempts to shut down the source VM before triggering the failover. Failover continues even if shutdown fails.
3. A test failover runs:
  - A prerequisites check runs to make sure all of the conditions required for migration are in place.
  - Failover processes the data so that an Azure VM can be created. If the latest recovery point is selected, a recovery point is created from the data.
  - An Azure VM is created by using the data processed in the previous step.
4. After the failover finishes, the replica Azure VM appears in the Azure portal. They check that the VM is the appropriate size, that it's connected to the right network, and that it's running.
5. After verifying, they clean up the failover, and record and save any observations.

### Run a failover

1. After verifying that the test failover worked as expected, they create a recovery plan for migration, and add `WEBVM` to the plan.

2. They run a failover on the plan. They select the latest recovery point. They specify that Azure Migrate should try to shut down the on-premises VM before triggering the failover.

3. After the failover, they verify that the Azure VM appears as expected in the Azure portal.

4. After verifying the VM in Azure, they complete the migration to finish the migration process, stop replication

for the VM, and stop Azure Migrate billing for the VM.

NAME	REPLICATION HEALTH	STATUS	ACTIVE LOCATION
WEBVM	-	Failover completed	<ul style="list-style-type: none"><li>Pin to dashboard </li><li>...</li><li>Failover</li><li>Test Failover</li><li>Cleanup test failover</li><li>Change recovery point</li><li>Commit</li><li>Complete Migration </li><li>Re-protect</li><li>Resynchronize</li><li>Error Details</li><li>Disable Replication</li></ul>

### Update the connection string

As the final step in the migration process, the Contoso admins update the connection string of the application to point to the migrated database running on the `SHAOG` listener. This configuration will be changed on the `WEBVM` now running in Azure. This configuration is located in the `web.config` of the ASP.NET application.

1. The Contoso admins locate the file at `C:\inetpub\SmartHotelWeb\web.config` and change the name of the server to reflect the FQDN of the Always On availability group: `shaog.contoso.com`.

```
<connectionStrings>
|   <add name="DefaultConnection" connectionString="Data Source=shaog.contoso.com;Database=SmartHotel.Registration"
|</connectionStrings>
```

2. After updating the file and saving it, they restart IIS on `WEBVM`. They use `iisreset /restart` from a command prompt.
3. After IIS is restarted, the application now uses the database running on the managed instance.

### Need more help?

- Learn about how to [run a test failover](#).
- Learn how to [create a recovery plan](#).
- Learn about [failing over to Azure](#).

### Clean up after migration

After migration, the SmartHotel360 application is running on an Azure VM. The SmartHotel360 database is located in the Azure SQL cluster.

Now, Contoso needs to finish these cleanup steps:

- Remove the on-premises VMs from the vCenter inventory.
- Remove the VMs from local backup jobs.
- Update internal documentation to show the new locations and IP addresses for VMs.
- Review any resources that interact with the decommissioned VMs. Update any relevant settings or documentation to reflect the new configuration.
- Add the two new VMs (`SQLAOG1` and `SQLAOG2`) to production monitoring systems.

### Review the deployment

With the migrated resources in Azure, Contoso needs to fully operationalize and secure its new infrastructure.

## Security

The Contoso security team reviews the virtual machines `WEBVM`, `SQLAOG1`, and `SQLAOG2` to determine any security issues. They need to:

- Review the network security groups (NSGs) for the VM to control access. NSGs are used to ensure that only traffic allowed to the application can pass.
- Consider securing the data on the disk by using Azure Disk Encryption and Azure Key Vault.
- Evaluate transparent data encryption. Then enable it on the SmartHotel360 database running on the new Always On availability group. Learn more about [transparent data encryption](#).

For more information, see [Security best practices for IaaS workloads in Azure](#).

## Business continuity and disaster recovery

For business continuity and disaster recovery, Contoso takes the following actions:

- To keep data safe, Contoso backs up the data on the `WEBVM`, `SQLAOG1`, and `SQLAOG2` VMs via [Azure VM backup](#).
- Contoso will also learn about how to use Azure Storage to back up SQL Server directly to Azure Blob storage. Learn more about how to [use Azure Storage for SQL Server backup and restore](#).
- To keep applications up and running, Contoso replicates the application VMs in Azure to a secondary region by using Site Recovery. Learn more about how to [set up disaster recovery to a secondary Azure region for an Azure VM](#).

## Licensing and cost optimization

- Contoso has existing licensing for its WEBVM and will take advantage of the Azure Hybrid Benefit. Contoso will convert the existing Azure VMs to take advantage of this pricing.
- Contoso will use [Azure Cost Management and Billing](#) to ensure the company stays within budgets established by the IT leadership.

## Conclusion

In this article, Contoso rehosted the SmartHotel360 application in Azure by migrating the application front-end VM to Azure by using Azure Migrate. Contoso migrated the application database to a SQL Server cluster provisioned in Azure by using Azure Database Migration Service and protected it in a SQL Server Always On availability group.

# Migrate open-source databases to Azure

11/9/2020 • 7 minutes to read • [Edit Online](#)

This article demonstrates how the fictional company Contoso assessed, planned, and migrated its various on-premises open-source databases to Azure.

As Contoso considers migrating to Azure, the company needs a technical and financial assessment to determine whether its on-premises workloads are good candidates for cloud migration. In particular, the Contoso team wants to assess machine and database compatibility for migration. Additionally, it wants to estimate capacity and costs for running Contoso's resources in Azure.

## Business drivers

Contoso is having various issues with maintaining the wide array of versions of open-source database workloads that exist on its network. After the latest investor's meeting, the CFO and CTO decided to move all these workloads to Azure. This move will shift them from a structured capital expense model to a fluid operating expense model.

The IT leadership team has worked closely with business partners to understand the business and technical requirements. They want to:

- **Increase security.** Contoso needs to be able to monitor and protect all data resources in a more timely and efficient manner. The company also wants to get a more centralized reporting system set up on database access patterns.
- **Optimize compute resources.** Contoso has deployed a large on-premises server infrastructure. The company has several SQL Server instances that consume but don't really use the underlying CPU, memory, and disk allocated in efficient ways.
- **Increase efficiency.** Contoso needs to remove unnecessary procedures and streamline processes for developers and users. The business needs IT to be fast and not waste time or money to deliver faster on customer requirements. Database administration should be reduced or minimized after the migration.
- **Increase agility.** Contoso IT needs to be more responsive to the needs of the business. It must react faster than the changes in the marketplace to enable success in a global economy. It mustn't get in the way or become a business blocker.
- **Scale.** As the business grows successfully, Contoso IT must provide systems that grow at the same pace.
- **Understand costs.** Business and application owners want to know they won't be stuck with high cloud costs when running the applications on-premises.

## Migration goals

The Contoso cloud team has pinned down goals for the various migrations. These goals were used to determine the best migration methods.

REQUIREMENTS	DETAILS
Performance	After migration, applications in Azure should have the same performance capabilities that applications have today in Contoso's on-premises environment. Moving to the cloud doesn't mean that application performance is less critical.

REQUIREMENTS	DETAILS
Compatibility	Contoso needs to understand the compatibility of its applications and databases with Azure. Contoso also needs to understand its Azure hosting options.
Data sources	All databases will be moved to Azure with no exceptions. Based on the database and application analysis of the SQL features being used, they'll move to platform as a service (PaaS) or infrastructure as a service (IaaS). All databases must move.
Application	Applications must be moved to the cloud wherever possible. If they can't move, they'll connect to the migrated database over the Azure network through private connections only.
Costs	Contoso wants to understand not only its migration options but also the costs associated with the infrastructure after it moves to the cloud.
Management	Resource management groups need to be created for the various departments along with resource groups to manage all databases that are migrated. All resources need to be tagged with department information for chargeback requirements.
Limitations	Initially, not all branch offices that run applications will have a direct Azure ExpressRoute link to Azure. These offices will need to connect through virtual network gateways.

## Solution design

Contoso has already performed a [migration assessment](#) of its digital estate by using [Azure Migrate](#).

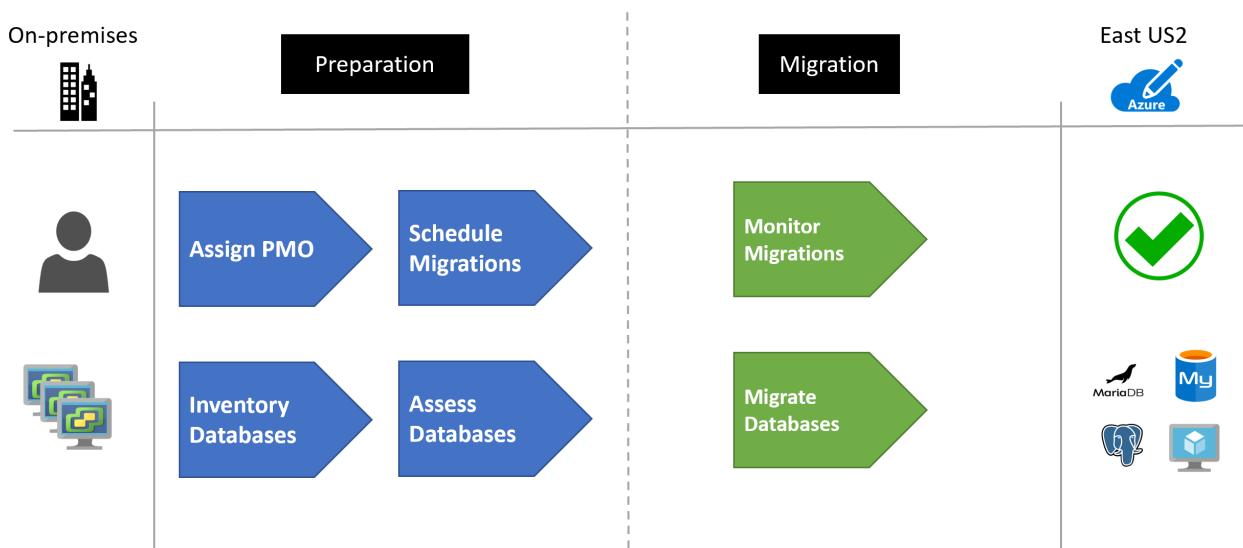


Figure 1: The migration process.

### Solution review

Contoso evaluates the proposed design by putting together a pros and cons list.

CONSIDERATION	DETAILS
<b>Pros</b>	<p>Azure will provide a single pane of glass into the database workloads.</p> <p>Costs will be monitored via Azure Cost Management + Billing.</p> <p>Business chargeback billing will be easy to perform with the Azure Billing APIs.</p> <p>Server and software maintenance will be reduced to only the IaaS-based environments.</p>
<b>Cons</b>	Because of the requirement of IaaS-based VMs, there will still be a need to manage the software on those machines.

### Budget and management

Before the migration can occur, the necessary Azure structure is required to be in place to support the administration and billing aspects of the solution.

For the management requirements, several [management groups](#) were created to support the organizational structure.

For the billing requirements, each of the Azure resources are then [tagged](#) with the appropriate billing tags.

### Migration process

Data migrations follow a standard and repeatable pattern. This process involves the following steps based on [Microsoft best practices](#):

- Pre-migration:
  - **Discovery:** Inventory database assets and application stack.
  - **Assess:** Assess workloads and fix recommendations.
  - **Convert:** Convert source schema to work in the target.
- Migration:
  - **Migrate:** Migrate the source schema, source data, and objects to target.
  - **Sync data:** Sync data (for minimal downtime).
  - **Cutover:** Cut over the source to target.
- Post-migration:
  - **Remediate applications:** Iteratively make any necessary changes to applications.
  - **Perform tests:** Iteratively run functional and performance tests.
  - **Optimize:** Based on tests, address performance issues and then retest to confirm performance improvements.
  - **Retire assets:** Old VMs and hosting environments are backed up and retired.

#### Step 1: Discovery

Contoso used Azure Migrate to surface the dependencies across the Contoso environment. Azure Migrate automatically discovered application components on Windows and Linux systems and mapped the communication between services. Azure Migrate also surfaced the connections between Contoso servers, processes, inbound and outbound connection latency, and ports across the TCP-connected architecture. Contoso was only required to install the [Microsoft Monitoring Agent](#) and the [Microsoft Dependency Agent](#).

Contoso has identified over 300 database instances that must be migrated. Of these instances, roughly 40 percent can be moved to PaaS-based services. Of the remaining 60 percent, they must be moved to an IaaS-based approach with a VM running the respective database software.

## **Step 2: Application assessment**

The results from the assessment showed Contoso that it uses primarily Java, PHP, and Node.js applications. The company has identified the following applications:

- 100 Java applications
- About 50 Node.js applications
- About 25 PHP applications

## **Step 3: Database assessment**

As the databases were inventoried, each type of database was reviewed to determine the method to migrate it to Azure. The following guidelines were followed on the database migrations.

DATABASE TYPE	DETAILS	TARGET	MIGRATION GUIDE
MySQL	All supported versions upgrade to a supported version before migration	Azure Database for MySQL (PaaS)	<a href="#">Guide</a>
PostgreSQL	All supported versions upgrade to a supported version before migration	Azure Database for PostgreSQL (PaaS)	<a href="#">Guide</a>
MariaDB	All supported versions upgrade to a supported version before migration	Azure Database for MariaDB (PaaS)	<a href="#">Guide</a>

## **Step 4: Migration planning**

Because of the large number of databases, Contoso set up a project management office to keep track of every database migration instance. [Accountability and responsibilities](#) were assigned to each business and application team.

Contoso also performed a [workload readiness review](#). This review examined the infrastructure, database, and network components.

## **Step 5: Test migrations**

The first part of the migration preparation involved a test migration of each of the databases to the pre-setup environments. To save time, Contoso scripted all of the operations for the migrations and recorded the timings for each. To speed up the migration, the company identified the migration operations that could run concurrently.

Any rollback procedures were identified for each of the database workloads in case of some unexpected failures.

For the IaaS-based workloads, the company set up all the required third-party software beforehand.

After the test migration, Contoso used the various Azure [cost-estimation tools](#) to get a more accurate picture of the future operational costs of the migration.

## **Step 6: Migration**

For the production migration, Contoso identified the time frames for all database migrations and what could be sufficiently executed in a weekend window (midnight Friday through midnight Sunday) with minimal downtime to the business.

## **Clean up after migration**

Contoso identified the archival window for all database workloads. As the window expires, the resources will be deallocated from the on-premises infrastructure. This process includes removing the production data from on-premises servers and retiring the hosting server when the last workload window expires.

## **Review the deployment**

With the migrated resources in Azure, Contoso needs to fully operationalize and secure its new infrastructure.

## Security

Contoso needs to:

- Ensure that its new Azure database workloads are secure. For more information, see [Azure SQL Database and SQL Managed Instance security capabilities](#).
- Review the firewall and virtual network configurations.
- Set up Azure Private Link so that all database traffic is kept inside Azure and the on-premises network.
- Enable Azure Advanced Threat Protection.

## Backups

Ensure that the Azure databases are backed up by using geo-restore. In this way, backups can be used in a paired region if a regional outage occurs.

### IMPORTANT

Make sure that the Azure resource has a [resource lock](#) to prevent it from being deleted. Deleted servers can't be restored.

## Licensing and cost optimization

- Many Azure database workloads can be scaled up or down. Monitoring server and database performance is important to ensure that you're meeting your needs and keeping costs at a minimum.
- Both CPU and storage have costs associated. There are several pricing tiers to select from. Make sure that the appropriate pricing plan is selected for the data workloads.
- Each read replica is billed based on the compute and storage selected.
- Use reserved capacity to reduce costs.

## Conclusion

In this article, Contoso assessed, planned, and migrated its open-source databases to Azure PaaS and IaaS solutions.

# Migrate MySQL databases to Azure

11/9/2020 • 7 minutes to read • [Edit Online](#)

This article demonstrates how the fictional company Contoso planned and migrated its on-premises MySQL open-source database platform to Azure.

## Business drivers

The IT leadership team has worked closely with business partners to understand what they want to achieve with this migration. They want to:

- **Increase availability.** Contoso has had availability issues with its MySQL on-premises environment. The business requires the applications that use this data store to be more reliable.
- **Increase efficiency.** Contoso needs to remove unnecessary procedures and streamline processes for developers and users. The business needs IT to be fast and not waste time or money to deliver faster on customer requirements.
- **Increase agility.** Contoso IT needs to be more responsive to the needs of the business. It must react faster than the changes in the marketplace to enable success in a global economy. It mustn't become a business blocker.
- **Scale.** As the business grows successfully, Contoso IT must provide systems that grow at the same pace.

## Migration goals

The Contoso cloud team has pinned down goals for this migration. These goals were used to determine the best migration method.

REQUIREMENTS	DETAILS
Availability	Currently internal staff are having a hard time with the hosting environment for the MySQL instance. Contoso wants to have close to 99.99 percent availability for the database layer.
Scalability	The on-premises database host is quickly running out of capacity. Contoso needs a way to scale its instances past current limitations or scale down if the business environment changes to save on costs.
Performance	The Contoso human resources (HR) department runs various reports daily, weekly, and monthly. When it runs these reports, it experiences significant performance issues with the employee-facing application. It needs to run the reports without affecting application performance.
Security	Contoso needs to know that the database is accessible only to its internal applications and isn't visible or accessible via the internet.
Monitoring	Contoso currently uses tools to monitor the metrics of the MySQL database server and provide notifications when CPU, memory, or storage have issues. The company wants to have this same capability in Azure.

Requirements	Details
Business continuity	The HR data store is an important part of Contoso's daily operations. If it became corrupted or needed to be restored, the company wants to minimize downtime as much as possible.
Azure	Contoso wants to move the application to Azure without running it on VMs. Contoso wants to use Azure platform as a service (PaaS) services for the data tier.

## Solution design

After pinning down goals and requirements, Contoso designs and reviews a deployment solution and identifies the migration process. The tools and services that it will use for migration are also identified.

### Current application

The MySQL database stores employee data that's used for all aspects of the company's HR department. A [LAMP-based](#) application is used as the front end to handle employee HR requests. Contoso has 100,000 employees worldwide, so uptime is important.

### Proposed solution

Use Azure Database Migration Service to migrate the database to an Azure Database for MySQL instance. Modify all applications and processes to use the new Azure Database for MySQL instance.

### Database considerations

As part of the solution design process, Contoso reviewed the features in Azure for hosting its MySQL data. The following considerations helped the company decide to use Azure:

- Similar to Azure SQL Database, Azure Database for MySQL allows for [firewall rules](#).
- Azure Database for MySQL can be used with [Azure Virtual Network](#) to prevent the instance from being publicly accessible.
- Azure Database for MySQL has the required compliance and privacy certifications that Contoso must meet for its auditors.
- Report and application processing performance will be enhanced by using read replicas.
- Ability to expose the service to internal network traffic only (no public access) by using [Azure Private Link](#).
- Contoso chose not to move to Azure Database for MySQL because it's considering using the MariaDB ColumnStore and graph database model in the future.
- Aside from MySQL features, Contoso is a proponent of true open-source projects and chose not to use MySQL.
- The [bandwidth and latency](#) from the application to the database will be sufficient enough based on the chosen gateway (either Azure ExpressRoute or Site-to-Site VPN).

### Solution review

Contoso evaluates the proposed design by putting together a pros and cons list.

Consideration	Details
---------------	---------

CONSIDERATION	DETAILS
Pros	<p>Azure Database for MySQL offers a 99.99 percent financially backed service-level agreement (SLA) for <a href="#">high availability</a>.</p> <p>Azure offers the ability to scale up or down during peak load times each quarter. Contoso can save even more by purchasing <a href="#">reserved capacity</a>.</p> <p>Azure provides point-in-time restore and geo-restore capabilities for Azure Database for MySQL.</p>
Cons	<p>Contoso is limited to the MySQL release versions that are supported in Azure, which are currently 10.2 and 10.3.</p> <p>Azure Database for MySQL has some <a href="#">limitations</a>, such as scaling down storage.</p>

## Proposed architecture

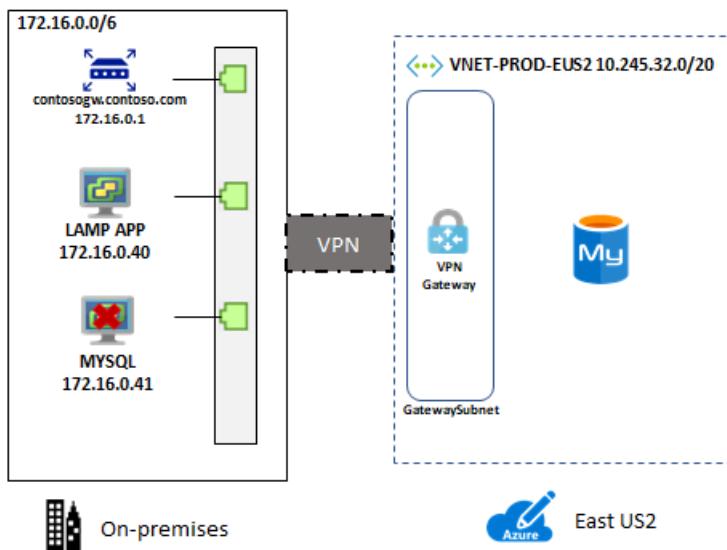


Figure 1: Scenario architecture.

### Migration process

#### Preparation

Before you can migrate your MySQL databases, you need to ensure that those instances meet all the Azure prerequisites for a successful migration.

#### Supported versions

MySQL uses the  $x.y.z$  versioning scheme, where  $x$  is the major version,  $y$  is the minor version, and  $z$  is the patch version.

Azure currently supports MySQL versions 10.2.25 and 10.3.16.

Azure automatically manages upgrades for patch updates. Examples are 10.2.21 to 10.2.23. Minor and major version upgrades aren't supported. For example, upgrading from MySQL 10.2 to MySQL 10.3 isn't supported. If you want to upgrade from 10.2 to 10.3, take a dump and restore it to a server created with the new engine version.

#### Network

Contoso needs to set up a virtual network gateway connection from its on-premises environment to the virtual network where its MySQL database is located. This connection allows the on-premises application to access the

database over the gateway when the connection strings are updated.

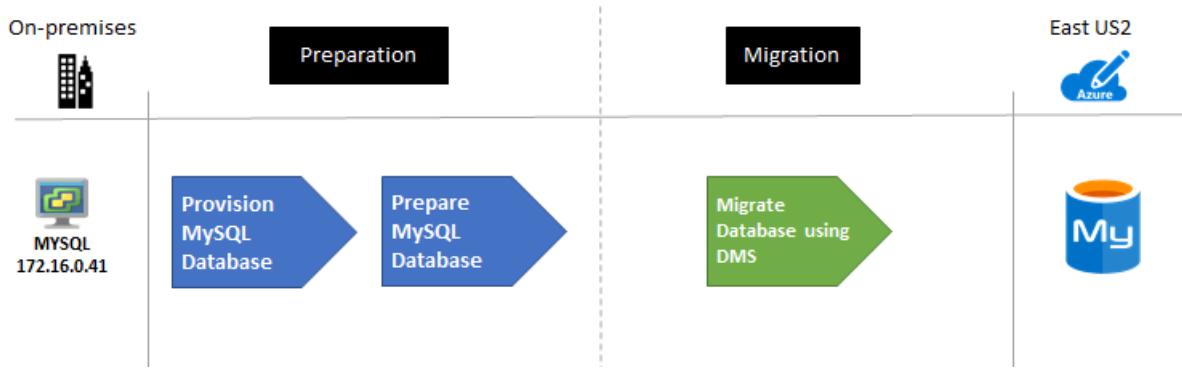


Figure 2: The migration process.

### Migration

Contoso admins migrate the database by using Azure Database Migration Service and following the [step-by-step migration tutorial](#). They can perform online, offline, and hybrid (preview) migrations by using MySQL 5.6 or 5.7.

#### NOTE

MySQL 8.0 is supported in Azure Database for MySQL. The Database Migration Service tool doesn't yet support that version.

As a summary, they must do the following tasks:

- Ensure all migration prerequisites are met:
  - The MySQL database server source must match the version that Azure Database for MySQL supports. Azure Database for MySQL supports MySQL Community Edition, the InnoDB storage engine, and migration across source and target with the same versions.
  - Enable binary logging in `my.ini` (Windows) or `my.cnf` (Unix). Failure to enable binary logging causes the following error in the Migration Wizard: "Error in binary logging. Variable binlog\_row\_image has value 'minimal.' please change it to 'full'." For more information, see the [MySQL documentation](#).
  - User must have the `ReplicationAdmin` role.
  - Migrate the database schemas without foreign keys and triggers.
- Create a virtual network that connects via ExpressRoute or a VPN to your on-premises network.
- Create an Azure Database Migration Service instance with a `Premium` SKU that's connected to the virtual network.
- Ensure that the instance can access the MySQL database via the virtual network. Make sure that all incoming ports are allowed from Azure to MySQL at the virtual network level, the network VPN, and the machine that hosts MySQL.
- Create a new Database Migration Service project:

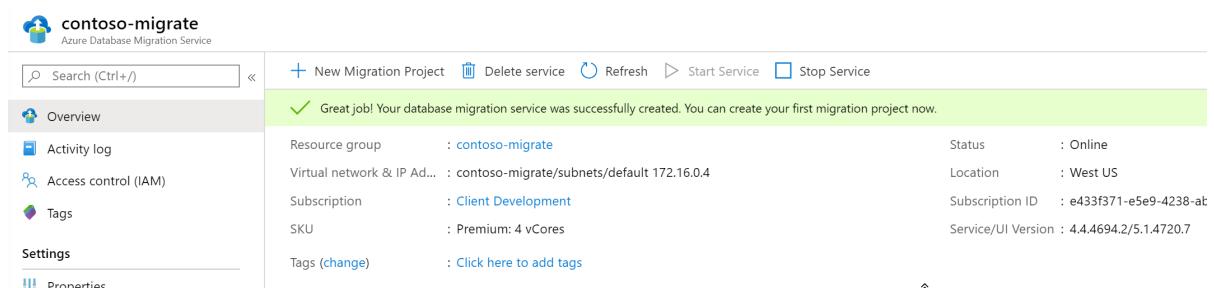


Figure 3: An Azure Database Migration Service project.

## Migration by using native tools

As an alternative to using Azure Database Migration Service, Contoso can use common utilities and tools such as MySQL Workbench, mysqldump, Toad, or Navicat to connect to and migrate data to Azure Database for MySQL.

- Dump and restore with mysqldump:
  - Use the exclude-triggers option in mysqldump to prevent triggers from executing during import and improve performance.
  - Use the single-transaction option to set the translation isolation mode to `REPEATABLE READ`, and send a `START TRANSACTION` SQL statement before you dump data.
  - Use the disable-keys option in mysqldump to disable foreign key constraints before load. Removing constraints provides performance gains.
  - Use Azure Blob storage to store the backup files and perform the restore from there for faster restore.
  - Update application connection strings.
  - After the database is migrated, Contoso must update the connection strings to point to the new Azure Database for MySQL.

## Clean up after migration

After migration, Contoso needs to back up the on-premises database for retention purposes and retire the on-premises MySQL database server.

## Review the deployment

With the migrated resources in Azure, Contoso needs to fully operationalize and secure its new infrastructure.

### Security

Contoso needs to:

- Ensure that its new Azure Database for MySQL instance and databases are secure. For more information, see [Security in Azure Database for MySQL](#).
- Review the firewall and virtual network configurations.
- Set up Private Link so that all database traffic is kept inside Azure and the on-premises network.
- Enable Azure Advanced Threat Protection.

### Backups

Ensure that the Azure Database for MySQL instances are backed up by using geo-restore, so that backups can be used in a paired region if a regional outage occurs.

#### IMPORTANT

Ensure that the Azure Database for MySQL resource has a resource lock to prevent it from being deleted. Deleted servers can't be restored.

### Licensing and cost optimization

- Azure Database for MySQL can be scaled up or down. Monitoring the performance of the server and databases is important to ensure your requirements are met while minimizing costs.
- Both CPU and storage have costs associated. Several pricing tiers are available. Be sure the appropriate pricing plan is selected for each data workload.
- Each read replica is billed based on the compute and storage selected.
- Use reserved capacity to save on costs.

## Conclusion

In this article, Contoso migrated its MySQL databases to an Azure Database for MySQL instance.

# Migrate PostgreSQL databases to Azure

11/9/2020 • 9 minutes to read • [Edit Online](#)

This article demonstrates how the fictional company Contoso planned and migrated its on-premises PostgreSQL open-source database platform to Azure.

## Business drivers

The IT leadership team has worked closely with business partners to understand what they want to achieve with this migration. They want to:

- **Automate big data.** Contoso uses PostgreSQL for several of its big data and AI initiatives. The company wants to build scalable repeatable pipelines to automate many of these analytical workloads.
- **Increase efficiency.** Contoso needs to remove unnecessary procedures and streamline processes for developers and users. The business needs IT to be fast and not waste time or money to deliver quicker on customer requirements.
- **Increase agility.** Contoso IT needs to be more responsive to the needs of the business. It must react faster than the changes in the marketplace to enable success in a global economy and to not become a business blocker.
- **Scale.** As the business grows successfully, Contoso IT must provide systems that can grow at the same pace.
- **Increase security.** Contoso realizes that regulatory issues will cause the company to adjust its on-premises strategy based on auditing, logging, and compliance requirements.

## Migration goals

The Contoso cloud team has pinned down goals for this migration and will use them to determine the best migration method.

REQUIREMENTS	DETAILS
Upgrades	Contoso wants to ensure that it has the latest patches installed when they're available, but the company doesn't want to manage these updates.
Integrations	Contoso wants to integrate the data in the database with data and AI pipelines for machine learning.
Backup and restore	Contoso is looking for the ability to do point-in-time restores when and if data updates fail or are corrupted for any reason.
Azure	Contoso wants to monitor system and fire alerts based on performance and security.
Performance	In some cases, Contoso will have parallel data processing pipelines in different geographic regions and must read data from those regions.

## Solution design

After pinning down goals and requirements, Contoso designs and reviews a deployment solution and identifies the migration process. The tools and services it will use for migration are also identified.

## Current environment

PostgreSQL 9.6.7 is running on a physical Linux machine (`sql-pg-01.contoso.com`) in the Contoso datacenter. Contoso already has an Azure subscription with a Site-to-Site VPN gateway to an on-premises datacenter network.

## Proposed solution

- Use Azure Database Migration Service to migrate the database to an Azure Database for PostgreSQL instance.
- Modify all applications and processes to use the new Azure Database for PostgreSQL instance.
- Build a new data processing pipeline using Azure Data Factory that connects to the Azure Database for PostgreSQL instance.

## Database considerations

As part of the solution design process, Contoso reviewed the features in Azure for hosting its PostgreSQL data. The following considerations helped the company decide to use Azure:

- Similar to Azure SQL Database, Azure Database for PostgreSQL supports firewall rules.
- Azure Database for PostgreSQL can be used with virtual networks to prevent the instance from being publicly accessible.
- Azure Database for PostgreSQL has the required compliance certifications that Contoso must meet.
- Integration with DevOps and Azure Data Factory will allow for automated data processing pipelines to be built.
- Processing performance can be enhanced by using read replicas.
- Support for bring your own key (BYOK) for data encryption.
- Ability to expose the service to internal network traffic only (no-public access) by using Azure Private Link.
- The [bandwidth and latency](#) from the application to the database will be sufficient enough based on the chosen gateway (either Azure ExpressRoute or Site-to-Site VPN).

## Solution review

Contoso evaluates its proposed design by putting together a list of pros and cons.

CONSIDERATION	DETAILS
Pros	All currently required and in-use features are available in Azure Database for PostgreSQL.
Cons	Contoso will still need to do manual migration from a major version of PostgreSQL.

## Proposed architecture

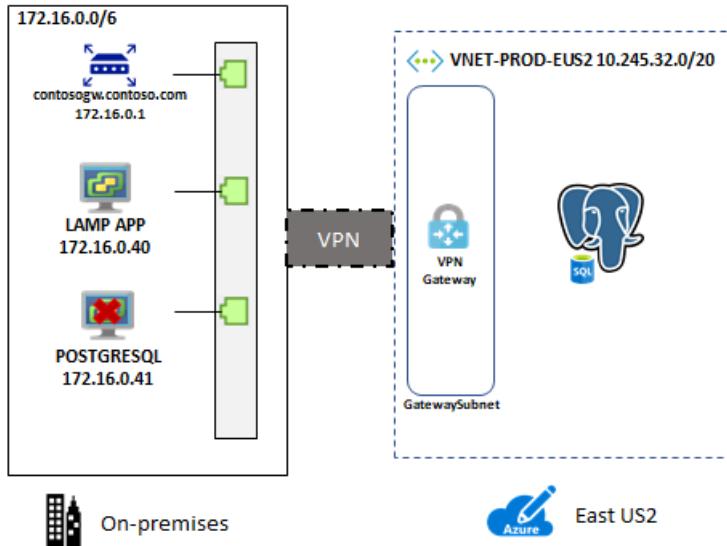


Figure 1: Scenario architecture.

## Migration process

### Preparation

Before Contoso can migrate its PostgreSQL databases, it ensures that Contoso's instances meet all the Azure prerequisites for a successful migration.

### Supported versions

Only migrations to the same or a higher version are supported. Migrating PostgreSQL 9.5 to Azure Database for PostgreSQL 9.6 or 10 is supported, but migrating from PostgreSQL 11 to PostgreSQL 9.6 isn't supported.

Microsoft aims to support  $n-2$  versions of the PostgreSQL engine in Azure Database for PostgreSQL - Single Server. The versions would be the current major version on Azure ( $n$ ) and the two prior major versions ( $-2$ ).

For the latest updates on supported versions, see [Supported PostgreSQL major versions](#).

### NOTE

Automatic major version upgrade isn't supported. For example, there isn't an automatic upgrade from PostgreSQL 9.5 to PostgreSQL 9.6. To upgrade to the next major version, dump the database and restore it to a server created with the target engine version.

### Network

Contoso will need to set up a virtual network gateway connection from its on-premises environment to the virtual network where its Azure Database for PostgreSQL database is located. This connection allows the on-premises application to access the database but not be migrated to the cloud.

### Assessment

Contoso will need to assess the current database for replication issues. These issues include:

- The source database version is compatible for migration to the target database version.
- Primary keys must exist on all tables to be replicated.
- Database names can't include a semicolon ( ; ).
- Migration of multiple tables with the same name, but a different case might cause unpredictable behavior.

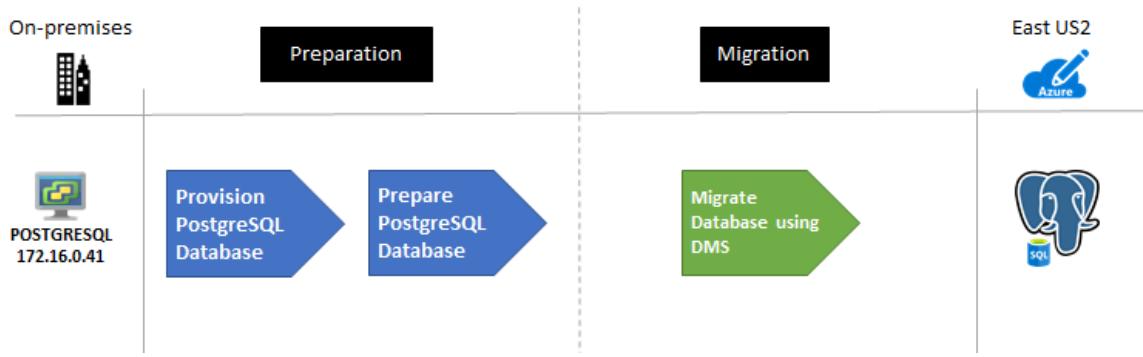


Figure 2: The migration process.

### Migration

Contoso can perform the migration in several ways:

- Dump and restore
- Azure Database Migration Service
- Import/export

Contoso has selected Azure Database Migration Service to allow the company to reuse the migration project whenever it needs to perform major-to-major upgrades. Because a single Database Migration Service activity only accommodates up to four databases, Contoso sets up several jobs by using the following steps.

To prepare, set up a virtual network to access the database. Create a virtual network connection by using [VPN gateways](#) in various ways.

### Create an Azure Database Migration Service instance

1. In the [Azure portal](#), select **Add a resource**.
2. Search for **Azure Database Migration Services**, and select it.
3. Select **+ Add**.
4. Select the subscription and resource group for the service.
5. Enter a name for the instance.
6. Select the closest location to the Contoso datacenter or VPN gateway.
7. Select **Azure** for the service mode.
8. Select a pricing tier.
9. Select **Review + create**.

## Create Migration Service

Basics Networking Tags Review + create

Azure Database Migration Service is designed to streamline the process of migrating on-premises databases to Azure.  
[Learn more.](#)

### Project details

Select the subscription to manage deployed resources and constants. Use resource groups as you would folders, to organize and manage all of your resources.

Subscription \* ⓘ

Client Development

Resource group \* ⓘ

cjg-migrate

[Create new](#)

### Instance details

Migration service name \* ⓘ

db-migration

Location \* ⓘ

(US) West US 2

Service mode \* ⓘ

Azure Hybrid (Preview)

Pricing tier \*

Standard

1 vCores

[Configure tier](#)

 Use an Azure Database Migration Service quick start template with pre-created source and targets. [Learn more.](#)

Figure 3: Review and create.

## 10. Select Create.

### Create an Azure Database for PostgreSQL instance

1. On the on-premises server, configure the `postgresql.conf` file.
  2. Set the server to listen on the proper IP address that Azure Database Migration Service will use to access the server and databases.
    - Set the `listen_addresses` variable.
  3. Enable SSL.
    - a. Set the `ssl=on` variable.
    - b. Verify that Contoso is using a publicly signed SSL certificate for the server that supports TLS 1.2. Otherwise, the Database Migration Service tool will raise an error.
  4. Update the `pg_hba.conf` file.
    - Add entries that are specific to the Database Migration Service instance.
5. Logical replication must be enabled on the source server by modifying the values in the `postgresql.conf` file for each server.
  - a. `wal_level = logical`
  - b. `max_replication_slots` = [at least the maximum number of databases for migration]
    - For example, if Contoso wants to migrate four databases, it sets the value to 4.
  - c. `max_wal_senders` = [number of databases running concurrently]

- The recommended value is 10.
- Migration **User** must have the **REPLICATION** role on the source database.
  - Add the Database Migration Service instance IP address to the **PostgreSQLPg\_hba.conf** file.
  - To export the database schemas, run the following commands:

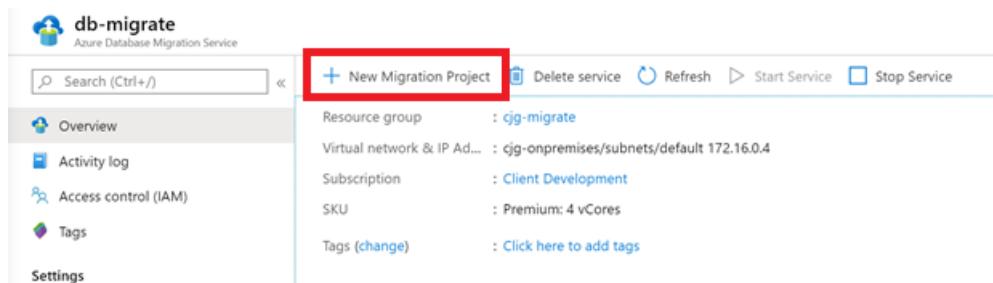
```
pg_dump -U postgres -s dvdrental > dvdrental_schema.sql
```

- Copy the file, name the copy **dvdrental\_schema\_foreign.sql**, and remove all non-foreign key and trigger-related items.
- Remove all foreign key and trigger-related items from the **dvdrental\_schema.sql** file.
- Import the database schema (step 1):

```
psql -h {host}.postgres.database.azure.com -d dvdrental -U username -f dvdrental_schema.sql
```

## Migration

- In the Azure portal, Contoso goes to its Database Migration Service resource.
- If the service isn't started, select **Start Service**.
- Select **New Migration Project**.



*Figure 4: Starting a new migration.*

- Select **New Activity > Online data migration**.
- Enter a name.
- Select **PostgreSQL** as the source.
- For the target, select **Azure Database for PostgreSQL** and then select **Save**.

# New migration project



Project name

postgres



Source server type \*

PostgreSQL



Target server type \*

Azure Database for PostgreSQL



\*Choose type of activity >

Online data migration

**To successfully use Database Migration Service (DMS) to migrate data, you need to:**

1. Migrate schema using pg\_dump -o -h hostname -U db\_username -d db\_name -s > your\_schema.sql
2. Remove foreign keys in schema at target Azure Database for PostgreSQL
3. Disable triggers at target Azure Database for PostgreSQL
4. Provision Database Migration Service and create a migration task

Please refer to [this tutorial](#) for more details.

*Figure 5: A new migration project is highlighted.*

8. Enter the source information, and select **Save**.

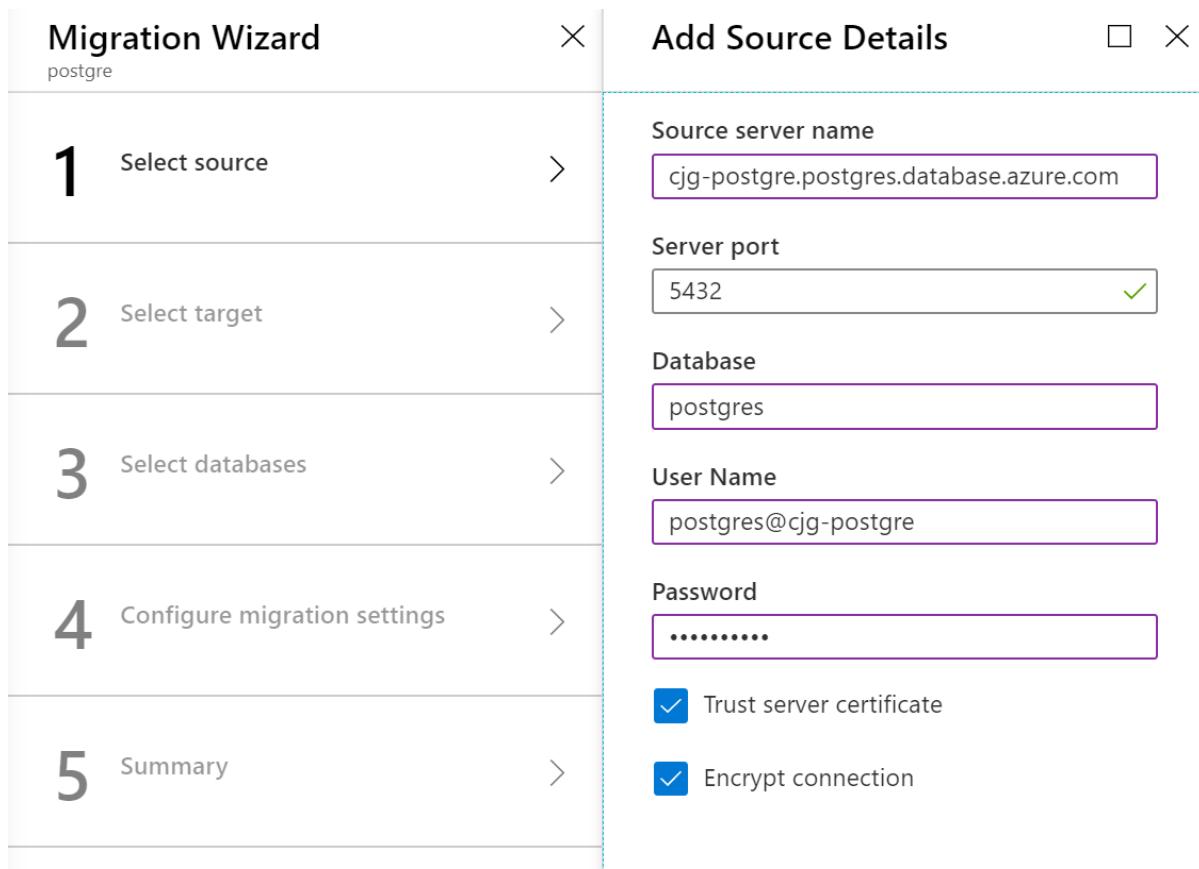


Figure 6: Entering source information.

9. Enter the target information, and select **Save**.

# Target details



## Subscription

Client Development



## Azure PostgreSQL

cjg-postgre



## Database

postgres

## User Name

postgres@cjg-postgre

## Password

••••••••••

Figure 7:

Selecting target information.

10. Select the databases to migrate. The schema for each database should have been migrated previously. Then select Save.

# Map to target databases



Search

All



2 item(s)

← prev

Page 1 of 1

next →



Source Database

Target Database



dvdrental

dvdrental



postgres

postgres



Figure 8: Selecting databases.

11. Configure the advanced settings, and select Save.

## Migration settings

The screenshot shows a hierarchical configuration interface. At the top level is a section for 'dvrental'. Below it is a section for 'Advanced online migration settings'. Within this section, there is a setting for 'Maximum number of tables to load in parallel' with a value of '5' entered into a text input field.

Figure 9: Configuring advanced settings.

12. Give the activity a name, and select Run.

The screenshot shows the 'Migration summary' interface. It includes fields for 'Activity name' (set to 'on-premises-one'), a warning message about truncation, and sections for 'Target server name' (set to 'cjg-postgre.postgres.database.azure.com'), 'Target server version' (set to 'Azure Database for PostgreSQL 10.11'), 'Source server name' (set to '52.191.131.189'), 'Source server version' (set to 'PostgreSQL 10.12'), and 'Database(s) to migrate' (set to '1 of 2').

Figure 10: Naming and running the activity.

13. Monitor the migration. Retry it if anything fails. An example is if foreign key references were missing.
14. After `Full load completed` matches the table count, select **Start Cutover**.

Source database name	Full load completed	Incremental updates	Pending changes
dvrental	15	0	0
Target database name	Full load queued	Incremental inserts	Applied changes
dvrental	0	0	0
Database status	Full load loading	Incremental deletes	Tables in error state
Running	0	0	0
Migration details	Full load failed		
Ready to cutover	0		

Figure 11: Monitoring the migration to start the cutover.

15. Stop all transactions from the source server.
16. Select the **Confirm** check box, and then select **Apply**.

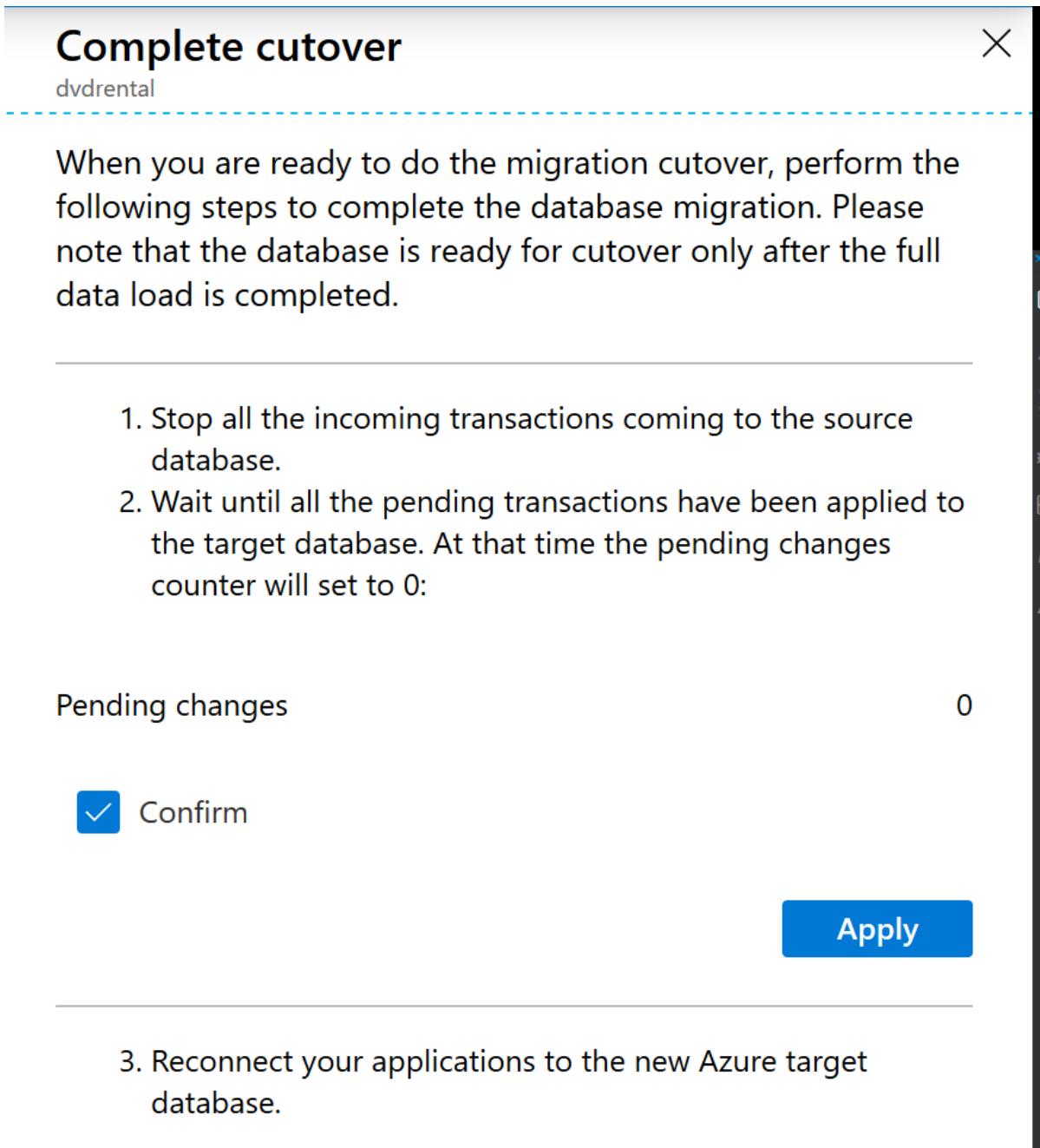


Figure 12: Running the cutover.

17. Wait for the cutover to complete.

Source server : 52.191.131.189  
Source version : PostgreSQL 10.12

Target server : cjg-postgre.postgres.database.azure.com  
Target version : Azure Database for PostgreSQL 10.11

**Migration Activities (4)**

Name	Activity Type	Status	Start Time
on-premises-one	Online data migration	Completed	03/20/2020, 1:24:58 PM
on-premises-one-01	Online data migration	Failed input validation	03/20/2020, 1:24:58 PM
on-premises-one-02	Online data migration	Failed input validation	03/20/2020, 1:24:58 PM
on-premises-one-03	Online data migration	Completed	03/20/2020, 1:24:58 PM

Figure 13: Completing the cutover.

#### NOTE

The previous Database Migration Service steps can also be performed via the [Azure CLI](#).

- Import the database schema (step 2):

```
psql -h {host}.postgres.database.azure.com -d dvdrental -U username -f dvdrental_schema_foreign.sql
```

- Reconfigure any applications or processes that use the on-premises database to point to the new Azure Database for PostgreSQL database instance.
- For post-migration, Contoso will ensure that it also set up cross-region read replicas, if necessary, after the migration is finished.

## Clean up after migration

After migration, Contoso needs to back up the on-premises database for retention purposes and retire the old PostgreSQL server as part of the cleanup process.

## Review the deployment

With the migrated resources in Azure, Contoso needs to fully operationalize and secure its new infrastructure.

### Security

Contoso needs to:

- Ensure that the new Azure Database for PostgreSQL instance and databases are secure. For more information, see [Security in Azure Database for PostgreSQL - Single Server](#).
- Review the [firewall rules](#) and virtual network configurations to verify that connections are limited to only the applications that require it.
- Implement [BYOK](#) for data encryption.
- Update all applications to [require SSL](#) connections to the databases.
- Set up [Private Link](#) so that all database traffic is kept inside Azure and the on-premises network.
- Enable [Azure Advanced Threat Protection \(ATP\)](#).
- Configure Log Analytics to monitor and alert on security and logs entries of interest.

### Backups

Ensure that the Azure Database for PostgreSQL databases is backed up by using geo-restore. In this way, backups can be used in a paired region if a regional outage occurs.

**IMPORTANT**

Make sure that the Azure Database for PostgreSQL resource has a resource lock to prevent it from being deleted. Deleted servers can't be restored.

## Licensing and cost optimization

- Azure Database for PostgreSQL can be scaled up or down. Performance monitoring of the server and databases is important to ensure that needs are met while keeping costs at a minimum.
- Both CPU and storage have costs associated. There are several pricing tiers to select from. Be sure the appropriate pricing plan is selected for the data workloads.
- Each read replica is billed based on the compute and storage selected.

## Conclusion

In this article, Contoso migrated its PostgreSQL databases to an Azure Database for PostgreSQL instance.

# Migrate MariaDB databases to Azure

11/9/2020 • 8 minutes to read • [Edit Online](#)

This article demonstrates how the fictional company Contoso planned and migrated its on-premises MariaDB open-source database platform to Azure.

Contoso is using MariaDB instead of MySQL because of its:

- Numerous storage engine options.
- Cache and index performance.
- Open-source support with features and extensions.
- ColumnStore storage engine for analytical workloads.

The company's migration goal is to continue to use MariaDB but not worry about managing the environment needed to support it.

## Business drivers

The IT leadership team has worked closely with business partners to understand what they want to achieve with this migration. They want to:

- **Increase availability.** Contoso has had availability issues with its MariaDB on-premises environment. The business requires the applications that use this data store to be more reliable.
- **Increase efficiency.** Contoso needs to remove unnecessary procedures and streamline processes for developers and users. The business needs IT to be fast and not waste time or money to deliver faster on customer requirements.
- **Increase agility.** Contoso IT needs to be more responsive to the needs of the business. It must react faster than the changes in the marketplace to enable success in a global economy. It mustn't get in the way or become a business blocker.
- **Scale.** As the business grows successfully, Contoso IT must provide systems that grow at the same pace.

## Migration goals

The Contoso cloud team has pinned down goals for this migration. These goals were used to determine the best migration method.

REQUIREMENTS	DETAILS
Availability	Currently internal staff are having a hard time with the hosting environment for the MariaDB instance. Contoso wants to have close to 99.99 percent availability for the database layer.
Scalability	The on-premises database host is quickly running out of capacity. Contoso needs a way to scale its instances past current limitations or scale down if the business environment changes to save on costs.

Requirements	Details
Performance	The Contoso human resources (HR) department has several reports it runs on a daily, weekly, and monthly basis. When it runs these reports, it notices considerable performance issues with the employee-facing application. It needs to run the reports without affecting application performance.
Security	Contoso needs to know that the database is accessible only to its internal applications and isn't visible or accessible via the internet.
Monitoring	Contoso currently uses tools to monitor the metrics of the MariaDB database and provide notifications when CPU, memory, or storage have issues. The company wants to have this same capability in Azure.
Business continuity	The HR data store is an important part of Contoso's daily operations. If it became corrupted or needed to be restored, the company wants to minimize downtime.
Azure	Contoso wants to move the application to Azure without running it on VMs. Contoso requirements state to use Azure platform as a service (PaaS) services for the data tier.

## Solution design

After pinning down goals and requirements, Contoso designs and reviews a deployment solution and identifies the migration process. The tools and services that it will use for migration are also identified.

### Current application

The MariaDB database hosts employee data that's used for all aspects of the company's HR department. A [LAMP-based](#) application is used as the front end to handle employee HR requests. Contoso has 100,000 employees worldwide, so uptime is important for its databases.

### Proposed solution

- Evaluate the environments for migration compatibility.
- Use common open-source tools to migrate databases to the Azure Database for MariaDB instance.
- Modify all applications and processes to use the new Azure Database for MariaDB instance.

### Database considerations

As part of the solution design process, Contoso reviewed the features in Azure for hosting its MariaDB databases. The following considerations helped the company decide to use Azure:

- Similar to Azure SQL Database, Azure Database for MariaDB allows for [firewall rules](#).
- Azure Database for MariaDB can be used with [Azure Virtual Network](#) to prevent the instance from being publicly accessible.
- Azure Database for MariaDB has the required compliance and privacy certifications that Contoso must meet for its auditors.
- Report and application processing performance will be enhanced by using read replicas.
- Ability to expose the service to internal network traffic only (no-public access) by using [Azure Private Link](#).
- Contoso chose not to move to Azure Database for MySQL because it's looking at potentially using the MariaDB ColumnStore and graph database model in the future.
- The [bandwidth and latency](#) from the application to the database will be sufficient enough based on the chosen

gateway (either Azure ExpressRoute or Site-to-Site VPN).

## Solution review

Contoso evaluates the proposed design by putting together a pros and cons list.

CONSIDERATION	DETAILS
Pros	<p>Azure Database for MariaDB offers a 99.99 percent financially backed service-level agreement (SLA) for <a href="#">high availability</a>.</p> <p>Azure offers the ability to scale up or down during peak load times each quarter. Contoso can save even more by purchasing <a href="#">reserved capacity</a>.</p> <p>Azure provides point-in-time restore and geo-restore capabilities for Azure Database for MariaDB.</p>
Cons	<p>Contoso is limited to the MariaDB release versions that are supported in Azure, which are currently 10.2 and 10.3.</p> <p>Azure Database for MariaDB has some <a href="#">limitations</a>, such as scaling down storage.</p>

## Proposed architecture

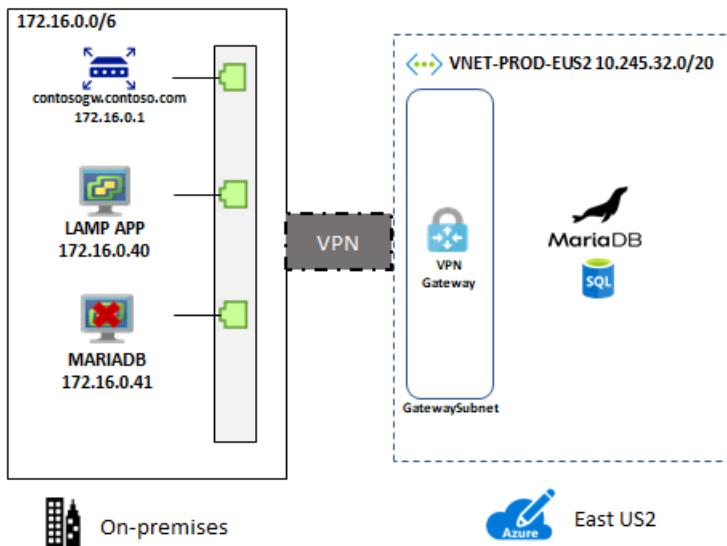


Figure 1: Scenario architecture.

## Migration process

### Preparation

Before you can migrate your MariaDB databases, you need to ensure that those instances meet all the Azure prerequisites for a successful migration.

Supported versions:

- MariaDB uses the x.y.z naming scheme. For example, x is the major version, y is the minor version, and z is the patch version.
- Azure currently supports 10.2.25 and 10.3.16.
- Azure automatically manages upgrades for patch updates. Examples are 10.2.21 to 10.2.23. Minor and major version upgrades aren't supported. For example, upgrading from MariaDB 10.2 to MariaDB 10.3 isn't supported. If you want to upgrade from 10.2 to 10.3, take a database dump and restore it to a server created with the target engine version.

The network:

Contoso needs to set up a virtual network gateway connection from its on-premises environment to the virtual network where its MariaDB database is located. This connection allows the on-premises application to access the database over the gateway when the connection strings are updated.

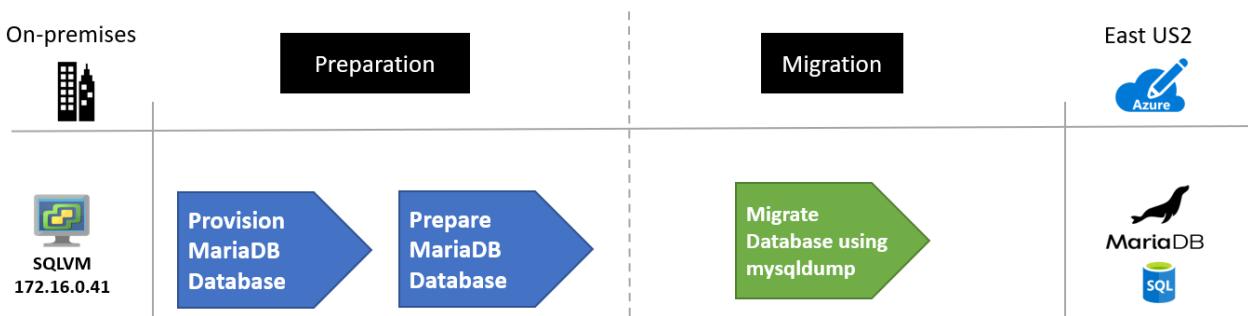


Figure 2: The migration process.

### Migration

Because MariaDB is similar to MySQL, Contoso can use the same common utilities and tools such as MySQL Workbench, mysqldump, Toad, or Navicat to connect to and migrate data to Azure Database for MariaDB.

Contoso used the following steps to migrate its databases.

- Determine the on-premises MariaDB version by running the following commands and observing the output. In most cases, your version shouldn't matter much for the schema and data dump. If you're using features at the application level, ensure those applications are compatible with the target version in Azure.

```
mysql -h localhost -u root -P
```

```
C:\Users\given>mysql -h localhost -u root -p
Enter password: *****
Welcome to the MariaDB monitor. Commands end with ; or \g.
Your MariaDB connection id is 13
Server version: 10.1.44-MariaDB mariadb.org binary distribution

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]>
```

Figure 3: Determining the on-premises MariaDB version.

- Create a new MariaDB instance in Azure:
  - Open the [Azure portal](#).
  - Select **Add a resource**.
  - Search for **MariaDB**.

Azure Database for MariaDB  
Microsoft



Azure Database for MariaDB

Microsoft

Save for later

Create

Overview Plans

Azure Database for MariaDB is a MariaDB database service built on Microsoft's scalable cloud infrastructure for application developers. Leverage your existing open-source MariaDB skills and tools and scale on-the-fly without downtime to efficiently deliver existing and new applications with reduced operational overhead. Built-in features maximize performance, availability, and security. Azure Database for MariaDB empowers developers to focus on application innovation instead of database management tasks.

Useful Links  
[Documentation](#)  
[Landing Page](#)  
[Pricing Details](#)

Figure 4: A new MariaDB instance in Azure.

- Select **Create**.
- Select your subscription and resource group.
- Select a server name and location.
- Select your target version, which is 10.2 or 10.3.
- Select your compute and storage.
- Enter an admin username and password.
- Select **Review + create**.

## Create MariaDB server

Microsoft

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription \* ⓘ

Client Development

Resource group \* ⓘ

cjg-migrate

[Create new](#)

### Server details

Enter required settings for this server, including picking a location and configuring the compute and storage resources.

Server name \* ⓘ

contoso-maria

Data source \* ⓘ

None  Backup

Location \* ⓘ

(US) West US 2

Version \* ⓘ

10.2

Compute + storage ⓘ

**General Purpose**

4 vCores, 100 GB storage

[Configure server](#)

### Administrator account

Admin username \* ⓘ

c2admin

Password \* ⓘ

••••••••••

Confirm password \*

••••••••••

[Review + create](#)

[Next : Tags >](#)

Figure 5: Review and create.

- Select **Create**.
- Record the server hostname, username, and password.
- Select **Connection Security**.
- Select **Add Client IP** (the IP that you'll be restoring the database from).
- Select **Save**.
- Run the following commands to export the database called `Employees`. Repeat for each database:

```
mysqldump -h localhost -u root -p --skip-triggers --single-transaction --extended-insert --order-by-primary --disable-keys Employees > Employees.sql
```

- Restore the database. Replace with the endpoint for your Azure Database for MariaDB instance and the username:

```
mysql -h {name}.mariadb.database.azure.com -u user@{name} -p -ssl
create database employees;
use database employees;
source employees.sql;
```

- Use phpMyAdmin or a similar tool, such as MySQL Workbench, Toad, and Navicat, to verify the restore by

checking record counts in each table.

- Update all application connection strings to point to the migrated database.
- Test all applications for proper operation.

## Clean up after migration

After a verified successful migration, Contoso needs to back up and store the on-premises database backup files for retention purposes. Retire the on-premises MariaDB server.

## Review the deployment

With the migrated resources in Azure, Contoso needs to fully operationalize and secure its new infrastructure.

### Security

Contoso needs to:

- Ensure that its new Azure Database for MariaDB instance and databases are secure. For more information, see [Security in Azure Database for MariaDB](#).
- Review the [firewall rules](#) and virtual network configurations to verify that connections are limited to only the applications that require it.
- Configure any outbound IP requirements to allow connections to the MariaDB [gateway IP addresses](#).
- Update all applications to [require SSL](#) connections to the databases.
- Set up [Private Link](#) so that all database traffic is kept inside Azure and the on-premises network.
- Enable [Azure Advanced Threat Protection \(ATP\)](#).
- Configure Log Analytics to monitor and send alerts on security and logs entries of interest.

### Backups

Ensure that the Azure Database for MariaDB instances are backed up by using geo-restore. In this way, backups can be used in a paired region if a regional outage occurs.

#### IMPORTANT

Make sure that the Azure Database for MariaDB instance has a [resource lock](#) to prevent it from being deleted. Deleted servers can't be restored.

### Licensing and cost optimization

- Azure Database for MariaDB can be scaled up or down. Performance monitoring of the server and databases is important to ensure you meet your needs but also keep costs at a minimum.
- Both CPU and storage have costs associated. There are several pricing tiers to select from. Be sure the appropriate pricing plan is selected for the data workloads.
- Each read replica is billed based on the compute and storage selected.
- Use reserved capacity to save on costs.

## Conclusion

In this article, Contoso migrated its MariaDB databases to an Azure Database for MariaDB instance.

# Rehost an on-premises Linux application to Azure VMs

11/9/2020 • 12 minutes to read • [Edit Online](#)

This article shows how the fictional company Contoso rehosts a two-tier [LAMP-based](#) application by using Azure infrastructure as a service (IaaS) virtual machines (VMs).

The service desk application used in this example, osTicket, is provided as open source. If you want to use it for your own testing purposes, you can download it from [GitHub](#).

## Business drivers

The IT leadership team has worked closely with business partners to understand what they want to achieve with this migration:

- **Address business growth.** Contoso is growing, and as a result there's pressure on the on-premises systems and infrastructure.
- **Limit risk.** The service desk application is critical for the Contoso business. Contoso wants to move it to Azure with zero risk.
- **Extend.** Contoso doesn't want to change the application right now. It wants to ensure that the application is stable.

## Migration goals

The Contoso cloud team has pinned down goals for this migration to determine the best migration method:

- After migration, the application in Azure should have the same performance capabilities as it does today in the company's on-premises VMware environment. The application will remain as critical in the cloud as it is on-premises.
- Contoso doesn't want to invest in this application. It's important to the business, but in its current form Contoso simply wants to move it safely to the cloud.
- Contoso doesn't want to change the ops model for this application. It wants to interact with the application in the cloud in the same way that it does now.
- Contoso doesn't want to change application functionality. Only the application location will change.
- Having completed a couple of Windows application migrations, Contoso wants to learn how to use a Linux-based infrastructure in Azure.

## Solution design

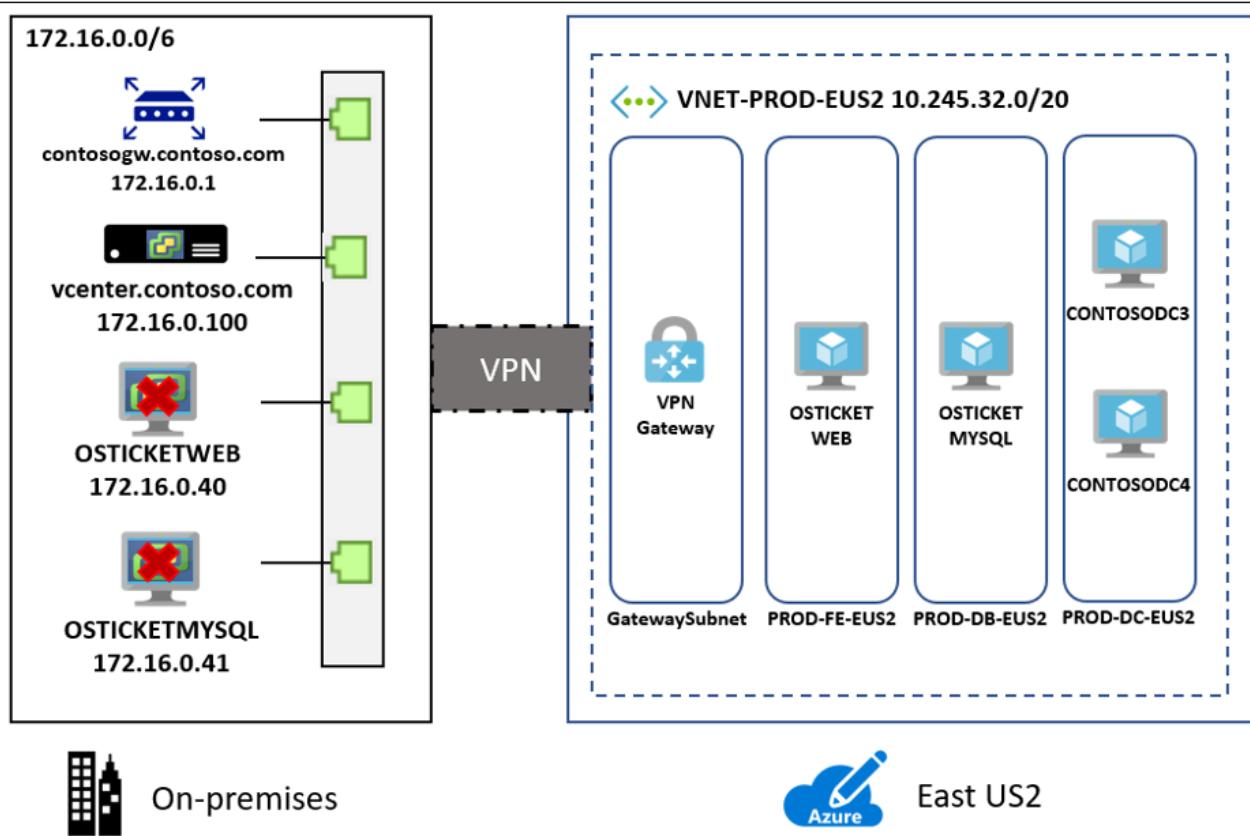
After pinning down goals and requirements, Contoso designs and reviews a deployment solution and identifies the migration process. The Azure services that Contoso will use for the migration also are identified.

### Current application

- The osTicket application is tiered across two VMs (`OSTICKETWEB` and `OSTICKETMYSQL`).
- The VMs are located on VMware ESXi host `contosohost1.contoso.com` (version 6.5).
- The VMware environment is managed by vCenter Server 6.5 (`vcenter.contoso.com`) and runs on a VM.
- Contoso has an on-premises datacenter (`contoso-datacenter`) with an on-premises domain controller (`contosodc1`).

## Proposed architecture

- Because the application is a production workload, the VMs in Azure will reside in the production resource group **ContosoRG**.
- The VMs will be migrated to the primary region (East US 2) and placed in the production network ( **VNET-PROD-EUS2** ):
  - The web VM will reside in the front-end subnet ( **PROD-FE-EUS2** ).
  - The database VM will reside in the database subnet ( **PROD-DB-EUS2** ).
- The on-premises VMs in the Contoso datacenter will be decommissioned after the migration is done.



## Solution review

Contoso evaluates the proposed design by putting together a list of pros and cons.

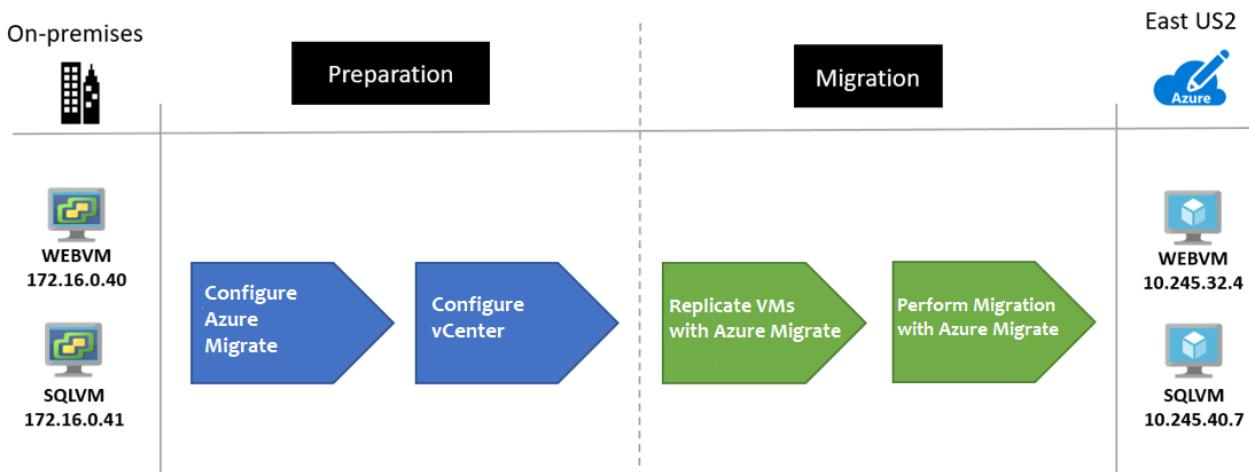
CONSIDERATION	DETAILS
<b>Pros</b>	<p>Both the application VMs will be moved to Azure without changes, which makes the migration simple.</p> <p>Because Contoso is using a lift-and-shift approach for both application VMs, no special configuration or migration tools are needed for the application database.</p> <p>Contoso will retain full control of the application VMs in Azure.</p> <p>The application VMs are running Ubuntu 16.04-TLS, an endorsed Linux distribution. Learn more about <a href="#">endorsed Linux distributions on Azure</a>.</p>

CONSIDERATION	DETAILS
Cons	<p>The web and data tier of the application remain single points of failover.</p> <p>Contoso will need to continue supporting the application as Azure VMs rather than moving to a managed service, such as Azure App Service and Azure Database for MySQL.</p> <p>Contoso realizes that by keeping things simple with a lift-and-shift VM migration, the company isn't taking full advantage of the features provided by <a href="#">Azure Database for MySQL</a>. These features include built-in high availability, predictable performance, simple scaling, automatic backups, and built-in security.</p>

## Migration process

Contoso will complete the migration process as follows:

- As a first step, Contoso prepares and sets up Azure components for Azure Migrate: Server Migration and prepares the on-premises VMware infrastructure.
- The company already has the [Azure infrastructure](#) in place, so it just needs to configure the replication of the VMs through the Azure Migrate: Server Migration tool.
- With everything prepared, Contoso can start replicating the VMs.
- After replication is enabled and working, Contoso will migrate the VM by failing it over to Azure.



## Azure services

SERVICE	DESCRIPTION	COST
Azure Migrate: Server Migration	The service orchestrates and manages migration of your on-premises applications and workloads and Amazon Web Services (AWS)/Google Cloud Platform (GCP) VM instances.	During replication to Azure, Azure Storage charges are incurred. Azure VMs are created, and incur charges, when migration occurs. Learn more about <a href="#">charges and pricing</a> .

## Prerequisites

Here's what Contoso needs for this scenario.

Requirements	Details
<b>Azure subscription</b>	<p>Contoso created subscriptions in an earlier article in this series. If you don't have an Azure subscription, create a <a href="#">free account</a>.</p> <p>If you create a free account, you're the administrator of your subscription and can perform all actions.</p> <p>If you use an existing subscription and you're not the administrator, work with the admin to assign you Owner or Contributor permissions.</p> <p>If you need more granular permissions, see <a href="#">Manage Azure Site Recovery access with role-based access control (RBAC)</a>.</p>
<b>Azure infrastructure</b>	<p>Learn how <a href="#">Contoso set up an Azure infrastructure</a>.</p> <p>Learn more about specific <a href="#">prerequisites</a> for Azure Migrate: Server Migration.</p>
<b>On-premises servers</b>	<p>The on-premises vCenter Server should be running version 5.5, 6.0, or 6.5.</p> <p>An ESXi host running version 5.5, 6.0, or 6.5.</p> <p>One or more VMware VMs running on the ESXi host.</p>
<b>On-premises VMs</b>	<p><a href="#">Review Linux Distros</a> that are endorsed to run on Azure.</p>

## Scenario steps

Here's how Contoso will complete the migration:

- **Step 1: Prepare Azure for Azure Migrate: Server Migration.** Add the Azure Migrate: Server Migration tool to the Azure Migrate project.
- **Step 2: Prepare on-premises VMware for Azure Migrate: Server Migration.** Prepare accounts for VM discovery, and prepare to connect to Azure VMs after migration.
- **Step 3: Replicate VMs.** Set up replication, and start replicating VMs to Azure Storage.
- **Step 4: Migrate the VMs with Azure Migrate: Server Migration.** Run a test migration to make sure everything's working, and then run a migration to move the VMs to Azure.

## Step 1: Prepare Azure for the Azure Migrate: Server Migration tool

Here are the Azure components Contoso needs to migrate the VMs to Azure:

- A virtual network in which Azure VMs will be located when they're created during migration.
- The Azure Migrate: Server Migration tool provisioned.

They set up these components as follows:

1. Set up a network. Contoso already set up a network that can be used for Azure Migrate: Server Migration when the company [deployed the Azure infrastructure](#)
  - The SmartHotel360 application is a production application. The VMs will be migrated to the Azure production network (`VNET-PROD-EUS2`) in the primary region (`East US 2`).
  - Both VMs will be placed in the `ContosoRG` resource group, which is used for production resources.

- The application front-end VM (`OSTICKETWEB`) will migrate to the front-end subnet (`PROD-FE-EUS2`) in the production network.
  - The application database VM (`OSTICKETMYSQL`) will migrate to the database subnet (`PROD-DB-EUS2`) in the production network.
2. Provision the Azure Migrate: Server Migration tool. With the network and storage account in place, Contoso now creates a Recovery Services vault (`ContosoMigrationVault`) and places it in the `ContosoFailoverRG` resource group in the primary region (`East US 2`).

Azure Migrate				
Azure Migrate				
Choose a tool to migrate your on-premises servers to Azure.				
TOOL	PRICING	SUPPORTED WORKLOADS	FEATURES	LEARN MORE
 <a href="#">Azure Migrate: Server Migration</a>	<a href="#">View</a>	VMware virtual machines Hyper-V virtual machines Physical machines Migration from other public clouds	Supports Windows and Linux Agentless and agent-based migration Cutover in seconds Minimal application downtime	<a href="#">Learn more</a>

### Need more help?

Learn about how to [set up the Azure Migrate: Server Migration tool](#).

## Step 2: Prepare on-premises VMware for Azure Migrate: Server Migration

After migration to Azure, Contoso wants to be able to connect to the replicated VMs in Azure. There are a couple of things that the Contoso admins need to do:

- To access Azure VMs over the internet, they enable SSH on the on-premises Linux VM before migration. For Ubuntu, this step can be completed by using the following command: `sudo apt-get ssh install -y`.
- Install the [Azure Linux agent](#)
- After they run the migration, they can check **Boot diagnostics** to view a screenshot of the VM.
- If it doesn't work, they'll need to check that the VM is running and review these [troubleshooting tips](#).

### Need more help?

Learn about how to [prepare VMs for migration](#).

## Step 3: Replicate the on-premises VMs

Before Contoso admins can run a migration to Azure, they need to set up and enable replication.

With discovery finished, begin replication of VMware VMs to Azure.

1. In the Azure Migrate project, go to **Servers > Azure Migrate: Server Migration**, and select **Replicate**.

The screenshot shows the Azure Migrate - Servers dashboard. On the left, there's a sidebar with navigation links: Overview, Migration goals, Servers (selected), Databases, Data Box, Manage, Discovered items, Support + troubleshooting, and New support request. The main area is titled 'Assessment tools' and contains a box for 'Azure Migrate: Server Assessment'. It has tabs for Discover, Assess, and Overview. Under Discover, it shows 442 Discovered servers, 2 Groups, 2 Assessments, and 0 Notifications. A callout says 'Next step: Start migrating your servers or optionally you can refine your application grouping with dependency analysis'. Below this is a link to 'Add more assessment tools? Click here.' Another box titled 'Migration tools' contains a 'Azure Migrate: Server Migration' section with tabs for Discover, Replicate (which is highlighted with a red box), Migrate, and Overview. It shows 442 Discovered servers.

2. In Replicate > Source settings > Are your machines virtualized?, select Yes, with VMware vSphere.
3. In On-premises appliance, select the name of the Azure Migrate appliance that you set up, and then select OK.

The screenshot shows the 'Replicate' configuration page. At the top, there are tabs for Source settings (selected), Virtual machines, Target settings, Compute, Disks, and Review + Start replication. Below the tabs, a note says: 'The first step in migrating servers is to replicate them. Once replication completes, you can perform test migration before finally moving the servers to Azure.' There are two required fields with dropdown menus: 'Are your machines virtualized?' (set to 'Yes, with VMware vSphere') and 'On-premises appliance' (set to '<appliance-name>').

4. In Virtual machines, select the machines you want to replicate.
  - If you've run an assessment for the VMs, you can apply VM sizing and disk type (premium/standard) recommendations from the assessment results. In Import migration settings from an Azure Migrate assessment?, select the Yes option.

- If you didn't run an assessment, or you don't want to use the assessment settings, select the **No** option.
- If you selected to use the assessment, select the VM group and assessment name.

The screenshot shows the 'Replicate' wizard interface. At the top, there are tabs: 'Source settings', 'Virtual machines' (which is underlined, indicating it's the active tab), 'Target settings', 'Compute', 'Disks', and 'Review + Start replication'. Below the tabs, a section titled 'Select the virtual machines to be migrated.' contains a note about importing migration settings from an assessment. A dropdown menu is open, showing two options: 'Yes, apply migration settings from a Azure Migrate assessment' and 'No, I'll specify the migration settings manually'. The 'Yes' option is highlighted with a blue background.

5. In **Virtual machines**, search for VMs as needed, and select each VM you want to migrate. Then select **Next: Target settings**.
6. In **Target settings**, select the subscription and target region to which you'll migrate. Specify the resource group in which the Azure VMs will reside after migration. In **Virtual Network**, select the Azure virtual network/subnet to which the Azure VMs will be joined after migration.
7. In **Azure Hybrid Benefit**:
  - Select **No** if you don't want to apply Azure Hybrid Benefit. Then select **Next**.
  - Select **Yes** if you have Windows Server machines that are covered with active Software Assurance or Windows Server subscriptions and you want to apply the benefit to the machines you're migrating. Then select **Next**.
8. In **Compute**, review the VM name, size, OS disk type, and availability set. VMs must conform with [Azure requirements](#).
  - **VM size:** If you're using assessment recommendations, the VM size drop-down list will contain the recommended size. Otherwise, Azure Migrate picks a size based on the closest match in the Azure subscription. Alternatively, pick a manual size in **Azure VM size**.
  - **OS disk:** Specify the OS (boot) disk for the VM. The OS disk is the disk that has the operating system bootloader and installer.
  - **Availability set:** If the VM should be in an Azure availability set after migration, specify the set. The set must be in the target resource group you specify for the migration.
9. In **Disks**, specify whether the VM disks should be replicated to Azure. Select the disk type (standard SSD/HDD or premium-managed disks) in Azure. Then select **Next**.
  - You can exclude disks from replication.
  - If you exclude disks, they won't be present on the Azure VM after migration.
10. In **Review + Start replication**, review the settings. Then select **Replicate** to start the initial replication for the servers.

#### **NOTE**

You can update replication settings any time before replication starts in **Manage > Replicating machines**. Settings can't be changed after replication starts.

## Step 4: Migrate the VMs

Contoso admins run a quick test migration and then a migration to move the VMs.

## Run a test migration

1. In Migration goals > Servers > Azure Migrate: Server Migration, select Test migrated servers.

The screenshot shows the 'Azure Migrate: Server Migration' dashboard. At the top, there are four navigation tabs: Discover, Replicate, Migrate, and Overview. Below the tabs, there is a summary table with four rows:

Category	Count
Discovered servers	442
Replicating servers	6
Test migrated servers	1
Migrated servers	1

Below the table, a note says: "Next step: You can start migrating the replicating servers to Azure". The 'Test migrated servers' row is highlighted with a red box.

2. Select and hold (or right-click) the VM to test. Then select **Test migrate**.

The screenshot shows the 'Replicating machines' blade in the Azure portal. On the left, there is a sidebar with options like Overview, Getting started, Migrate servers to Azure, Manage, and Replicating machines. Under Replicating machines, it lists 'Jobs' and 'Events'. The main area shows a table with one row:

NAME	STATUS	HEALTH	MIGRATION PHASE	LAST SYNC	TEST MIGRATION STATUS
Contoso-Win2K8R2SP1	Delta sync	Healthy	Test migration pending	2/17/2019, 12:00:43 AM	Never performed

A context menu is open over the first row, with the 'Test migrate' option highlighted by a red box.

3. In **Test Migration**, select the Azure virtual network in which the Azure VM will be located after the migration. We recommend you use a nonproduction virtual network.
4. The **Test migration** job starts. Monitor the job in the portal notifications.
5. After the migration finishes, view the migrated Azure VM in **Virtual Machines** in the Azure portal. The machine name has a suffix **-Test**.
6. After the test is done, select and hold (or right-click) the Azure VM in **Replicating machines**. Then select **Clean up test migration**.

The screenshot shows the 'Replicating machines' blade again. The context menu for the same VM (Contoso-Win2K8R2SP1) is open, and the 'Clean up test migration' option is highlighted with a red box.

## Migrate the VMs

Now Contoso admins run a full migration to complete the move.

1. In the Azure Migrate project, go to **Servers > Azure Migrate: Server Migration**, and select **Replicating servers**.

The screenshot shows the 'Migration tools' interface for 'Azure Migrate: Server Migration'. The 'Overview' tab is active. The main content area displays four categories with counts: 'Discovered servers' (58), 'Replicating servers' (1), 'Test migrated servers' (0), and 'Migrated servers' (0). A red box highlights the 'Replicating servers' row. At the bottom, a note reads: 'Next step: You can start migrating the replicating servers to Azure'.

2. In **Replicating machines**, select and hold (or right-click) the VM and select **Migrate**.
3. In **Migrate > Shut down virtual machines and perform a planned migration with no data loss**, select **Yes > OK**.
  - By default, Azure Migrate shuts down the on-premises VM and runs an on-demand replication to synchronize any VM changes that occurred since the last replication occurred. This action ensures no data loss.
  - If you don't want to shut down the VM, select **No**.
4. A migration job starts for the VM. Track the job in Azure notifications.
5. After the job finishes, you can view and manage the VM from the **Virtual Machines** page.

#### Connect the VM to the database

As the final step in the migration process, Contoso admins update the connection string of the application to point to the application database running on the **OSTICKETWEB** VM.

1. Make an SSH connection to the **OSTICKETWEB** VM by using PuTTY or another SSH client. The VM is private, so connect by using the private IP address.

## Connect to virtual machine



OSTICKETWEB

RDP

SSH

To connect to your virtual machine via SSH, select an IP address, optionally change the port number, and use one of the following commands:

\* IP address

Private IP address (10.245.32.5)



\* Port number

22

Login using VM local account

ssh <Login username>@10.245.32.5



```
$ ssh contosoadmin@10.245.32.5
The authenticity of host '10.245.32.5 (10.245.32.5)' can't be established.
ECDSA key fingerprint is SHA256:aJNt+VbYqoZb+mrB1CCj5
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.245.32.5' (ECDSA) to the list of known hosts.
contosoadmin@10.245.32.5's password:
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.4.0-127-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

136 packages can be updated.
59 updates are security updates.

Last login: [REDACTED] from 172.16.0.200
contosoadmin@osticketweb:~$ |
```

2. Make sure that the `OSTICKETWEB` VM can communicate with the `OSTICKETMYSQL` VM. Currently, the configuration is hardcoded with the on-premises IP address `172.16.0.43`.

Before the update:

```
# Database Options
# -----
# Mysql Login info
define('DBTYPE', 'mysql');
define('DBHOST', '172.16.0.43');
define('DBNAME', 'osticket');
define('DBUSER', 'osticket');
```

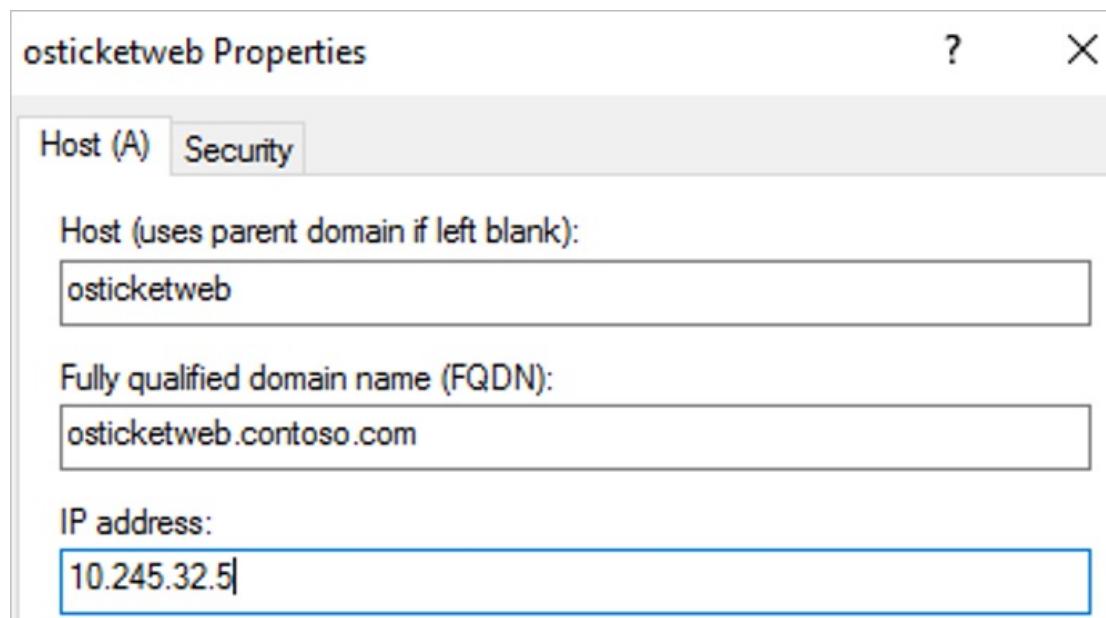
After the update:

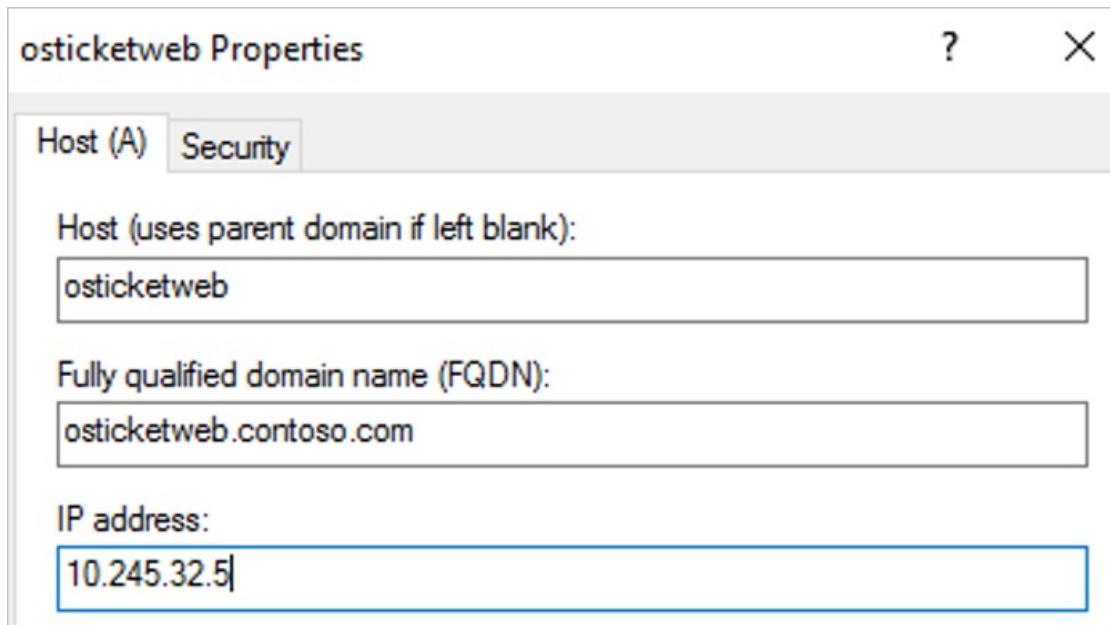
```
# Database Options
# -----
# Mysql Login info
define('DBTYPE', 'mysql');
define('DBHOST', 'osticketmysql.contoso.com');
define('DBNAME', 'osticket');
define('DBUSER', 'osticket');
-- INSERT --
```

3. Restart the service with `systemctl restart apache2`.

```
contosoadmin@osticketweb:~$ systemctl restart apache2
===== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units
Authentication is required to restart 'apache2.service'.
Authenticating as: contosoadmin,,,(contosoadmin)
Password:
===== AUTHENTICATION COMPLETE ===
contosoadmin@osticketweb:~$
```

4. Finally, update the DNS records for `OSTICKETWEB` and `OSTICKETMYSQL` on one of the Contoso domain controllers.





#### Need more help?

- Learn about how to [run a test migration](#).
- Learn about how to [migrate VMs to Azure](#).

## Clean up after migration

With migration complete, the osTicket application tiers are now running on Azure VMs.

Now, Contoso needs to do the following tasks:

- Remove the on-premises VMs from the vCenter inventory.
- Remove the on-premises VMs from local backup jobs.
- Update the internal documentation to show the new location and IP addresses for **OSTICKETWEB** and **OSTICKETMYSQL**.
- Review any resources that interact with the VMs. Update any relevant settings or documentation to reflect the new configuration.
- Contoso used the Azure Migrate service with management VM to assess the VMs for migration. Admins should remove the migration VM and web VMs from VMware ESXi server.

## Review the deployment

With the application now running, Contoso needs to fully operationalize and secure its new infrastructure.

### Security

The Contoso security team reviews the OSTICKETWEB and OSTICKETMYSQL VMs to determine any security issues.

- The team reviews the network security groups (NSGs) for the VMs to control access. NSGs are used to ensure that only traffic allowed to the application can pass.
- The team also considers securing the data on the VM disks by using Azure Disk Encryption and Azure Key Vault.

For more information, see [Security best practices for IaaS workloads in Azure](#).

### Business continuity and disaster recovery

For business continuity and disaster recovery, Contoso takes the following actions:

- **Keep data safe.** Contoso backs up the data on the VMs by using [Azure VM backup](#).
- **Keep applications up and running.** Contoso replicates the application VMs in Azure to a secondary region

by using Site Recovery. For more information, see [Quickstart: Set up disaster recovery to a secondary Azure region for an Azure VM](#).

#### Licensing and cost optimization

- After deploying resources, Contoso assigns Azure tags as defined during the [Azure infrastructure deployment](#).
- Contoso has no licensing issues with the Ubuntu servers.
- Contoso will use [Azure Cost Management and Billing](#) to ensure the company stays within budgets established by the IT leadership.

# Rehost an on-premises Linux application to Azure VMs and Azure Database for MySQL

11/9/2020 • 15 minutes to read • [Edit Online](#)

This article shows how the fictional company Contoso rehosts a two-tier [LAMP-based](#) application and migrates it from on-premises to Azure by using Azure Virtual Machines (VMs) and Azure Database for MySQL.

The service desk application used in this example, osTicket, is provided as open source. If you want to use it for your own testing, you can download it from [GitHub](#).

## Business drivers

The IT leadership team has worked closely with business partners to understand what they want to achieve:

- **Address business growth.** Contoso is growing, and as a result there's pressure on the on-premises systems and infrastructure.
- **Limit risk.** The service desk application is critical for the business. Contoso wants to move it to Azure with zero risk.
- **Extend.** Contoso doesn't want to change the application right now. The company wants to keep the application stable.

## Migration goals

The Contoso cloud team has pinned down goals for this migration to determine the best migration method:

- After migration, the application in Azure should have the same performance capabilities as it does today in the company's on-premises VMware environment. The application will remain as critical in the cloud as it is on-premises.
- Contoso doesn't want to invest in this application. It's important to the business, but in its current form Contoso simply wants to move it safely to the cloud.
- Having completed a couple of Windows application migrations, Contoso wants to learn how to use a Linux-based infrastructure in Azure.
- Contoso wants to minimize database admin tasks after the application is moved to the cloud.

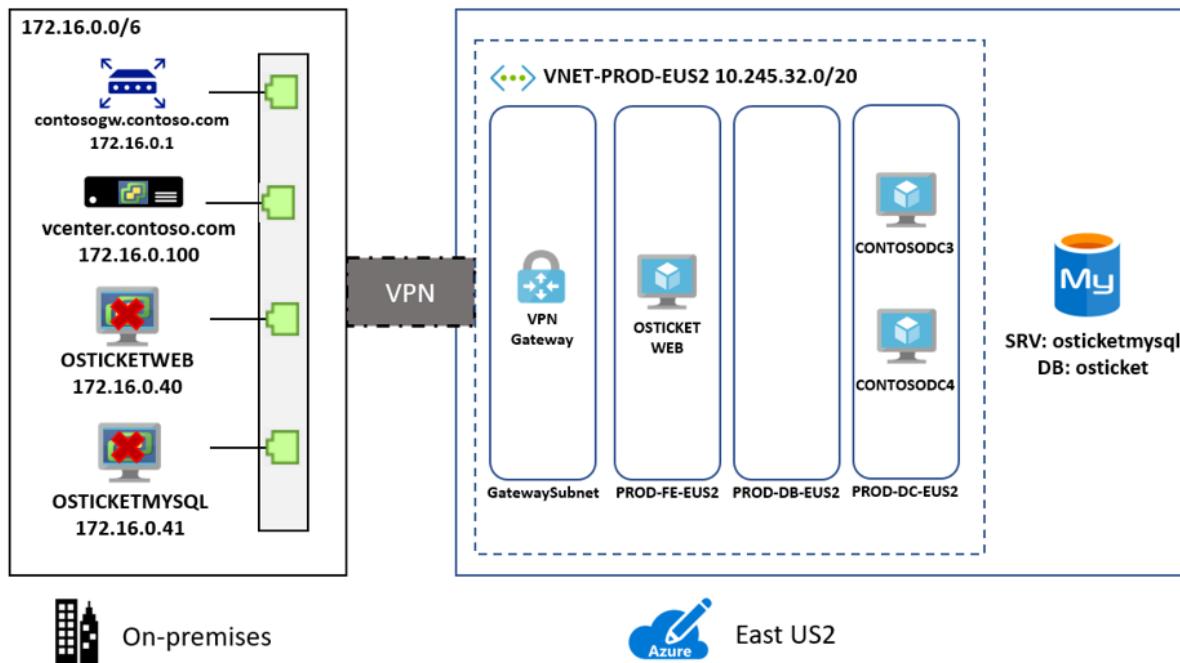
## Proposed architecture

In this scenario:

- Currently the application is tiered across two VMs (`OSTICKETWEB` and `OSTICKETMYSQL`).
- The VMs are located on VMware ESXi host `contosohost1.contoso.com` (version 6.5).
- The VMware environment is managed by vCenter Server 6.5 (`vcenter.contoso.com`) and runs on a VM.
- Contoso has an on-premises datacenter (`contoso-datacenter`), with an on-premises domain controller (`contosodc1`).
- The web application on `OSTICKETWEB` will be migrated to an Azure infrastructure as a service (IaaS) VM.
- The application database will be migrated to the Azure Database for MySQL platform as a service.
- Because Contoso is migrating a production workload, the resources will reside in the production resource

group ContosORG .

- The `OSTICKETWEB` resource will be replicated to the primary region (East US 2) and placed in the production network (`VNET-PROD-EUS2`):
  - The web VM will reside in the front-end subnet (`PROD-FE-EUS2`).
- The application database will be migrated to Azure Database for MySQL by using [Azure Database Migration Service](#).
- The on-premises VMs in the Contoso datacenter will be decommissioned after the migration is done.



## Migration process

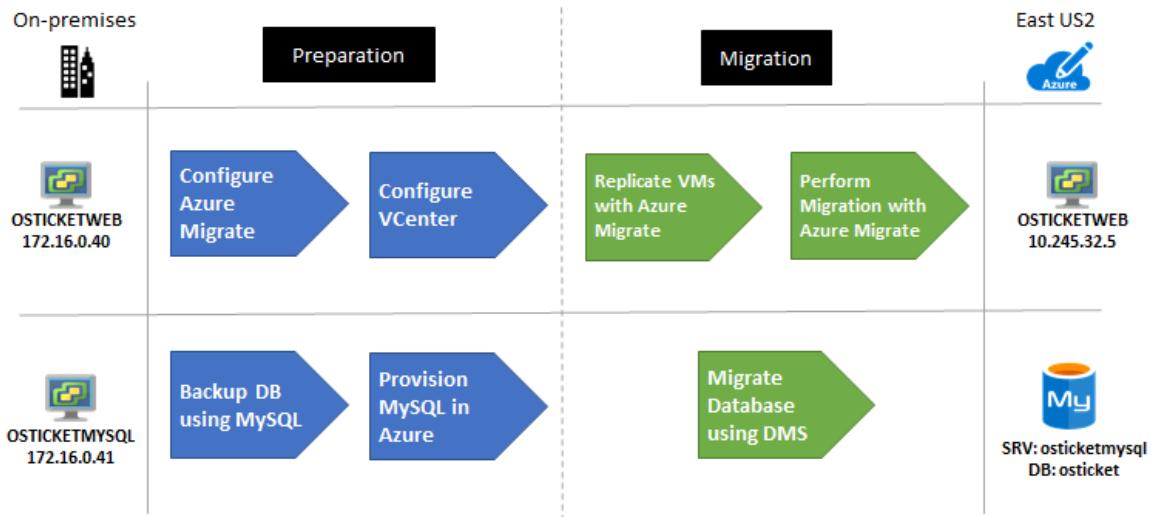
Contoso will complete the migration process as follows:

To migrate the web VM:

- As a first step, Contoso sets up the Azure and on-premises infrastructure needed to deploy Azure Migrate.
- The company already has the [Azure infrastructure](#) in place, so it just needs to add and configure the replication of the VMs through the Azure Migrate: Server Migration tool.
- With everything prepared, Contoso can start replicating the VM.
- After replication is enabled and working, Contoso will complete the move by using Azure Migrate.

To migrate the database:

1. Contoso provisions a MySQL instance in Azure.
2. Contoso sets up Database Migration Service, ensuring access to the on-premises database server.
3. Contoso migrates the database to Azure Database for MySQL.



## Azure services

SERVICE	DESCRIPTION	COST
Azure Migrate	Contoso uses Azure Migrate to assess its VMware VMs. Azure Migrate assesses the migration suitability of the machines. It provides sizing and cost estimates for running in Azure.	Azure Migrate is available at no additional charge. You might incur charges depending on the tools (first-party or ISV) you decide to use for assessment and migration.
Azure Database Migration Service	Database Migration Service enables seamless migration from multiple database sources to Azure data platforms with minimal downtime.	Learn about <a href="#">supported regions</a> and <a href="#">Database Migration Service pricing</a> .
Azure Database for MySQL	The database is based on the open-source MySQL database engine. It provides a fully managed enterprise-ready community MySQL database for application development and deployment.	Learn more about Azure Database for MySQL <a href="#">pricing</a> and scalability options.

## Prerequisites

Here's what Contoso needs for this scenario.

REQUIREMENTS	DETAILS
Azure subscription	<p>Contoso created subscriptions during an earlier article. If you don't have an Azure subscription, create a <a href="#">free account</a>.</p> <p>If you create a free account, you're the administrator of your subscription and can perform all actions.</p> <p>If you use an existing subscription and you're not the administrator, work with the admin to assign you Owner or Contributor permissions.</p> <p>If you need more granular permissions, see <a href="#">Manage Azure Site Recovery access with role-based access control (RBAC)</a>.</p>

Requirements	Details
Azure infrastructure	Contoso set up the Azure infrastructure as described in <a href="#">Azure infrastructure for migration</a> .
On-premises servers	<p>The on-premises vCenter Server should be running version 5.5, 6.0, 6.5, or 6.7.</p> <p>An ESXi host running version 5.5, 6.0, 6.5, or 6.7.</p> <p>One or more VMware VMs running on the ESXi host.</p>
On-premises VMs	<a href="#">Review Linux machines</a> that are endorsed to run on Azure.

## Scenario steps

Here's how Contoso admins will complete the migration:

- **Step 1: Prepare Azure for Azure Migrate: Server Migration.** Add the server migration tool to the Azure Migrate project.
- **Step 2: Prepare on-premises VMware for Azure Migrate: Server Migration.** Prepare accounts for VM discovery and prepare to connect to Azure Virtual Machines after migrated.
- **Step 3: Replicate VMs.** Set up replication and start replicating VMs to Azure Storage.
- **Step 4: Migrate the application VM with Azure Migrate: Server Migration.** Run a test migration to make sure everything's working, and then run a full migration to move the VM to Azure.
- **Step 5: Migrate the database.** Set up migration by using Azure Database Migration Service.

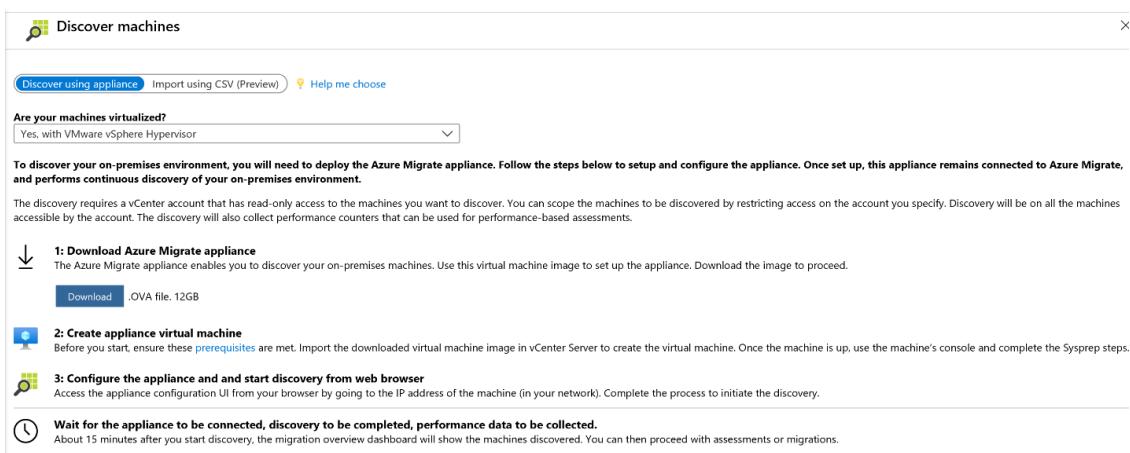
## Step 1: Prepare Azure for the Azure Migrate: Server Migration tool

Here are the Azure components Contoso needs to migrate the VMs to Azure:

- A virtual network in which Azure VMs will be located when they're created during migration.
- The Azure Migrate: Server Migration tool (OVA) provisioned and configured.

To set up the components, Contoso admins follow these steps:

1. Set up a network. Contoso already set up a network that can be used for Azure Migrate: Server Migration when it [deployed the Azure infrastructure](#).
2. Provision the Azure Migrate: Server Migration tool.
  - a. From Azure Migrate, download the OVA image, and import it into VMware.



b. Start the imported image, and configure the tool by using the following steps:

a. Set up the prerequisites.

Azure Migrate Appliance

### Set up discovery for Azure Migrate

Azure Migrate appliance helps you discover, assess and migrate your VMware virtual machines. Complete the following steps to initiate discovery. [Learn more](#) about Azure Migrate discovery capabilities.

 Set up prerequisites  
Verify and set up appliance prerequisites

  Accept license terms [View terms of use](#)

  Use of the Azure Migrate Appliance (the "software") is licensed to you as part of your or your company's subscription for the Azure Migrate Service (the "service"). Your use of the software is governed by the agreement under which you or your company obtained the service (see [Azure Legal Information](#)). Microsoft assumes no responsibility or liability whatsoever for any non-Microsoft product made available to you through your use of the service or software. Customer is solely responsible for any non-Microsoft product that it installs or uses with the service or software and acknowledges that use shall be governed by the separate agreement(s) between Customer and the publisher of the non-Microsoft product. See [TPN](#) for third-party components included in the software.

  Check connectivity to the Internet [Set up proxy](#)

  Check time is in sync with the Internet time server

  Check if latest Azure Migrate updates are installed

  Install VMware vSphere Virtual Disk Development Kit

[Continue](#)

 Register with Azure Migrate  
Specify your Microsoft Azure account details

b. Point the tool to the Azure subscription.

## Set up discovery for Azure Migrate

Azure Migrate appliance helps you discover, assess and migrate your VMware virtual machines. Complete the following steps to initiate discovery. [Learn more](#) about Azure Migrate discovery capabilities.



### Set up prerequisites

Verify and set up appliance prerequisites



### Register with Azure Migrate

Specify your Microsoft Azure account details



Choose the subscription and resource group that you used to set up Azure Migrate. The discovery and assessment metadata will be stored in the geography you selected while setting up Azure Migrate on the Azure portal. [Learn more](#)

Logged in as [REDACTED]

[Logout](#)

Subscription

Migrate project

Enter Appliance Name



[Register](#)

[Continue](#)

### c. Set the VMware vCenter credentials.



#### Specify vCenter Server

Provide vCenter Server details to discover machines. You can also choose to provide VM credentials for discovery of applications and dependencies.



Specify vCenter Server details and credentials

vCenter Server name/IP

Port

User name

Password

[Validate connection](#)

Successfully connected to vCenter Server

What metadata is discovered and what is it used for? [Learn more](#)

### d. Add any Linux-based credentials for discovery.

Discover applications and dependencies on VMs

Provide VM credentials for discovery of applications and for dependency analysis on the machines. Ensure 'Guest Operations' privileges are enabled for these VMs. [Learn more](#) about permissions.

The credentials will be saved on the appliance in an encrypted format. The discovery of applications and dependencies is done remotely without the installation of any agent or script on VMs.

[Add credentials](#)

Skip addition of VM credentials. You will not be able to discover applications and dependencies.  
Added credentials

OS Type	Friendly Name	Action
Windows	basic	<a href="#">Edit</a>
Linux	basic-linux	<a href="#">Edit</a>

[Save and start discovery](#)

- After the tool is configured, it takes some time for the tool to enumerate all the virtual machines. After the process is finished, the VMs populate in the Azure Migrate tool in Azure.

#### Need more help?

Learn about how to set up the [Azure Migrate: Server Migration tool](#).

## Step 2: Prepare on-premises VMware for Azure Migrate: Server Migration

After migrating to Azure, Contoso wants to be able to connect to the replicated VMs in Azure. There are a couple of things that the Contoso admins need to do:

- To access Azure VMs, they enable SSH on the on-premises Linux VM before migration. For Ubuntu, this step can be completed by using the following command: `sudo apt-get ssh install -y`.
- After the admins run the migration, they can check **boot diagnostics** to view a screenshot of the VM.
- If it doesn't work, they'll need to check that the VM is running, and review these [troubleshooting tips](#).
- Install the [Azure Linux agent](#).

#### Need more help?

Learn about how to [prepare VMs for migration](#).

## Step 3: Replicate VMs

Before Contoso admins can run a migration to Azure, they need to set up and enable replication.

With discovery finished, they can begin replication of the application VM to Azure.

- In the Azure Migrate project, go to **Servers > Azure Migrate: Server Migration**, and select **Replicate**.

The screenshot shows the Azure Migrate - Servers dashboard. On the left, there's a navigation sidebar with links for Overview, Migration goals, Servers (which is selected), Databases, Data Box, Manage (with Discovered items, Support + troubleshooting, and New support request), and a bottom section for adding more assessment tools.

**Assessment tools**

**Azure Migrate: Server Assessment**

- Discover
- Assess
- Overview

Category	Count
Discovered servers	442
Groups	2
Assessments	2
Notifications	0

**Next step:** Start migrating your servers or optionally you can refine your application grouping with dependency analysis

Add more assessment tools? [Click here.](#)

**Migration tools**

**Azure Migrate: Server Migration**

- Discover
- Replicate
- Migrate
- Overview

Category	Count
Discovered servers	442

2. In Replicate > Source settings > Are your machines virtualized?, select Yes, with VMware vSphere.
3. In On-premises appliance, select the name of the Azure Migrate appliance that you set up, and then select OK.

**Replicate**

Source settings Virtual machines Target settings Compute Disks Review + Start replication

The first step in migrating servers is to replicate them. Once replication completes, you can perform test migration before finally moving the servers to Azure.

\* Are your machines virtualized? [?](#)  
Yes, with VMware vSphere

\* On-premises appliance [?](#)  
<appliance-name>

4. In Virtual machines, select the machines you want to replicate:
  - If you've run an assessment for the VMs, you can apply VM sizing and disk type (premium/standard) recommendations from the assessment results. In Import migration settings from an Azure Migrate assessment?, select the Yes option.

- If you didn't run an assessment, or you don't want to use the assessment settings, select the **No** option.
- If you selected to use the assessment, select the VM group and assessment name.

The screenshot shows the 'Replicate' wizard interface. At the top, there are tabs: 'Source settings', 'Virtual machines' (which is selected), 'Target settings', 'Compute', 'Disks', and 'Review + Start replication'. Below the tabs, a section titled 'Select the virtual machines to be migrated.' contains a note about importing migration settings from an assessment. A dropdown menu is open, showing two options: 'Yes, apply migration settings from a Azure Migrate assessment' and 'No, I'll specify the migration settings manually'. The 'Yes' option is highlighted with a blue background.

5. In **Virtual machines**, search for VMs as needed, and select each VM you want to migrate. Then select **Next: Target settings**.
6. In **Target settings**, select the subscription and target region to which you'll migrate. Specify the resource group in which the Azure VMs will reside after migration. In **Virtual Network**, select the Azure virtual network/subnet to which the Azure VMs will be joined after migration.
7. In **Azure Hybrid Benefit**:
  - Select **No** if you don't want to apply Azure Hybrid Benefit. Then select **Next**.
8. In **Compute**, review the VM name, size, OS disk type, and availability set. VMs must conform with [Azure requirements](#).
  - **VM size:** If you use assessment recommendations, the VM size drop-down list contains the recommended size. Otherwise, Azure Migrate picks a size based on the closest match in the Azure subscription. Alternatively, pick a manual size in **Azure VM size**.
  - **OS disk:** Specify the OS (boot) disk for the VM. The OS disk is the disk that has the operating system bootloader and installer.
  - **Availability set:** If the VM should be in an Azure availability set after migration, specify the set. The set must be in the target resource group you specify for the migration.
9. In **Disks**, specify whether the VM disks should be replicated to Azure. Then select the disk type (standard SSD/HDD or premium-managed disks) in Azure, and select **Next**.
  - You can exclude disks from replication.
  - If you exclude disks, they won't be present on the Azure VM after migration.
10. In **Review + Start replication**, review the settings. Then select **Replicate** to start the initial replication for the servers.

#### **NOTE**

You can update replication settings any time before replication starts in **Manage > Replicating machines**. Settings can't be changed after replication starts.

## Step 4: Migrate the VM with Azure Migrate: Server Migration

Contoso admins run a quick test migration and then a full migration to move the web VM.

### Run a test migration

1. In **Migration goals > Servers > Azure Migrate: Server Migration**, select **Test migrated servers**.

## Migration tools

Azure Migrate: Server Migration

Discover   Replicate   Migrate   Overview

Discovered servers	442
Replicating servers	6
Test migrated servers	1
Migrated servers	1

**Next step:** You can start migrating the replicating servers to Azure

2. Select and hold (or right-click) the VM to test, and then select **Test migrate**.

NAME	STATUS	HEALTH	MIGRATION PHASE	LAST SYNC	TEST MIGRATION STATUS
Contoso-Win2K8R2SP1	Delta sync	Healthy	Test migration pending	2/17/2019, 12:00:43 AM	Never performed

Pin to dashboard     
 Test migrate   
 Clean up test migration   
 Migrate

3. In **Test Migration**, select the Azure virtual network in which the Azure VM will be located after the migration. We recommend you use a nonproduction virtual network.
4. The **Test migration** job starts. Monitor the job in the portal notifications.
5. After the migration finishes, view the migrated Azure VM in **Virtual Machines** in the Azure portal. The machine name has a suffix **-Test**.
6. After the test is done, select and hold (or right-click) the Azure VM in **Replicating machines**. Then select **Clean up test migration**.

NAME	STATUS	HEALTH	MIGRATION PHASE	LAST SYNC	TEST MIGRATION STATUS
Contoso-Win2K8R2SP1	Delta sync	Healthy	Test clean up pending	2/17/2019, 12:00:43 AM	2/17/2019, 10:02:30 AM

Pin to dashboard     
 Test migrate   
 Clean up test migration   
 Migrate   
 Error Details

## Migrate the VM

Now Contoso admins run a full migration to complete the move.

1. In the Azure Migrate project, go to **Servers > Azure Migrate: Server Migration**, and select Replicating servers.

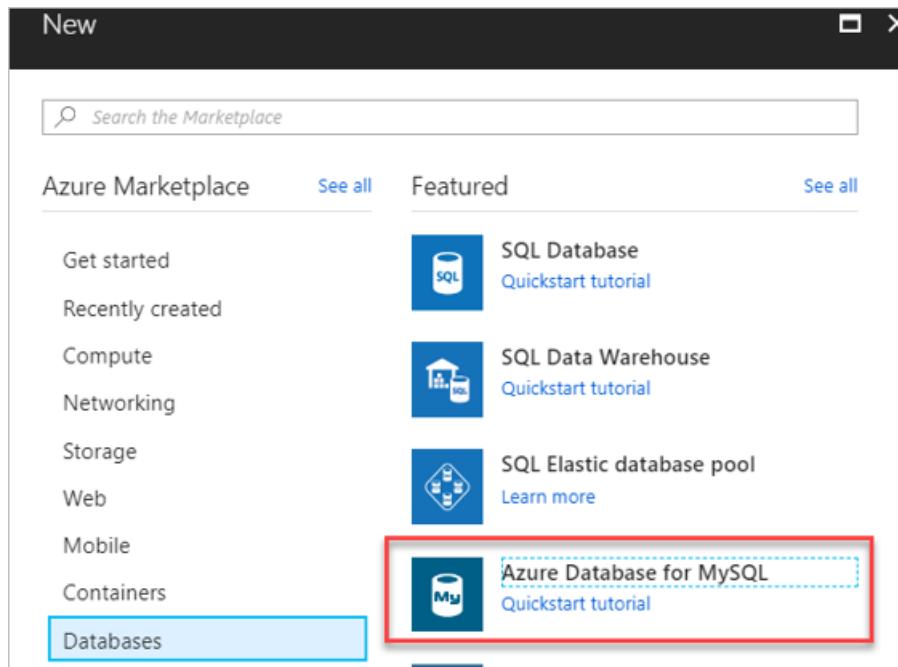
The screenshot shows the 'Migration tools' interface for 'Azure Migrate: Server Migration'. At the top, there are four tabs: 'Discover', 'Replicate', 'Migrate', and 'Overview', with 'Overview' being the active tab. Below the tabs, there are four categories: 'Discovered servers' (58), 'Replicating servers' (1, highlighted with a red box), 'Test migrated servers' (0), and 'Migrated servers' (0). A note at the bottom says: '⚡ Next step: You can start migrating the replicating servers to Azure'.

2. In **Replicating machines**, select and hold (or right-click) the VM, and then select **Migrate**.
3. In **Migrate > Shut down virtual machines and perform a planned migration with no data loss**, select **Yes > OK**.
  - By default, Azure Migrate shuts down the on-premises VM and runs an on-demand replication to synchronize any VM changes that occurred since the last replication occurred. This action ensures no data loss.
  - If you don't want to shut down the VM, select **No**.
4. A migration job starts for the VM. Track the job in Azure notifications.
5. After the job finishes, you can view and manage the VM from the **Virtual Machines** page.

## Step 5: Provision Azure Database for MySQL

Contoso admins provision a MySQL database instance in the primary region (`East US 2`).

1. In the Azure portal, create an Azure Database for MySQL resource.



2. Add the name `contosoosticket` for the Azure database. Add the database to the production resource group `ContosoRG`, and specify credentials for it.
3. The on-premises MySQL database is version 5.7, so select this version for compatibility. Use the default sizes, which match database requirements.

This screenshot shows the 'MySQL server' configuration dialog. The 'Name' field is set to 'contosoosticket'. Under 'Subscription', the 'Subscription' dropdown is expanded to show '<subscription id>'. Under 'Resource group', the 'Resource group' dropdown is expanded to show 'ContosoRG' with the 'Use existing' radio button selected. Under 'Select source', the 'Select source' dropdown is expanded to show 'Blank'. Under 'Server admin login name', the value 'contosoadmin' is entered. Under 'Password' and 'Confirm password', two masked password fields are shown, both with green checkmarks indicating they are valid. Under 'Location', 'East US 2' is selected. Under 'Version', '5.7' is selected. At the bottom, under 'Pricing tier', the text 'General Purpose, 2 vCore(s), 5 ...' is visible, followed by a right-pointing arrow.

4. For **Backup Redundancy Options**, select **Geo-Redundant**. This option allows you to restore the database in the secondary region (`Central US`) if an outage occurs. You can configure this option only when you

provision the database.

Backup Redundancy Options - [Learn more details](#)

**Locally Redundant**  
Recover from data loss  
within region

**Geo-Redundant**   
Recover from regional  
outage or disaster

5. In the `VNET-PROD-EUS2` network, go to **Service endpoints**, and add a service endpoint (a database subnet) for the SQL service.

Add service endpoints X

Service ▼  
Microsoft.Sql

\* Subnets ▼  
PROD-DB-EUS2

6. After adding the subnet, create a virtual network rule that allows access from the database subnet in the production network.

Create virtual network rule

\* Name VNET-PROD-EUS2-PROD-DB-EUS2 ✓ provide vnet rule name

\* Subscription Azure Migrate Program Management Team (8c3c936a-c09b-4de...

\* Virtual network VNET-PROD-EUS2

\* Subnet name / Address prefix PROD-DB-EUS2 / 10.245.40.0/23

VIRTUAL NETWORK		SERVICE ENDPOINT STATUS		
VNET-PROD-EUS2/PROD-DB-EUS2		Enabled		
VNET Rules	+ Adding existing virtual network	+ Create new virtual network		
RULE NAME	VIRTUAL NETWORK	SUBNET	ADDRESS RANGE	ENDPOINT STATUS
VNET-PROD-EUS2-PRO...	VNET-PROD-EUS2	PROD-DB-EUS2	10.245.40.0/23	Enabled

## Step 6: Migrate the database

There are several ways to move the MySQL database. Each option requires the Contoso admins to create an Azure Database for MySQL instance for the target. After it's created, they can perform the migration by using two paths that are described in the following steps:

- 6a: Database Migration Service
- 6b: MySQL Workbench backup and restore

### Step 6a: Migrate the database via Database Migration Service

Contoso admins migrate the database via Database Migration Service by following the [step-by-step migration tutorial](#). They can perform online, offline, and hybrid (preview) migrations by using MySQL 5.6 or 5.7.

#### NOTE

MySQL 8.0 is supported in Azure Database for MySQL, but the Database Migration Service tool doesn't yet support that version.

As a summary, Contoso admins must perform the following tasks:

- Ensure all migration prerequisites are met:
  - The MySQL server database source must match the version that Azure Database for MySQL supports. Azure Database for MySQL supports MySQL Community Edition, the InnoDB storage engine, and migration across the source and target with the same versions.
  - Enable binary logging in `my.ini` (Windows) or `my.cnf` (Unix). Failure to do so will cause the following error in the Migration Wizard: "Error in binary logging. Variable binlog\_row\_image has value 'minimal.' Please change it to 'full.'" For more information, see the [MySQL website](#).

- User must have `ReplicationAdmin` role.
- Migrate the database schemas without foreign keys and triggers.
- Create a virtual network that connects via Azure ExpressRoute or a VPN to your on-premises network.
- Create a Database Migration Service instance by using a `Premium` SKU that's connected to the virtual network.
- Ensure that the instance can access the MySQL database via the virtual network. Ensure that all incoming ports are allowed from Azure to MySQL at the virtual network level, the network VPN, and the machine that hosts MySQL.
- Run the Database Migration Service tool:
  - Create a migration project.

The screenshot shows the Azure Database Migration Service 'Overview' page for a service named 'contoso-migrate'. The left sidebar includes links for Overview, Activity log, Access control (IAM), Tags, Settings, and Properties. The main content area has a search bar and several navigation buttons: New Migration Project, Delete service, Refresh, Start Service, and Stop Service. A prominent green success message states: 'Great job! Your database migration service was successfully created. You can create your first migration project now.' Below this message, detailed service information is listed:

Resource group	: contoso-migrate	Status	: Online
Virtual network & IP Ad...	: contoso-migrate/subnets/default 172.16.0.4	Location	: West US
Subscription	: Client Development	Subscription ID	: e43f371-e5e9-4238-a...
SKU	: Premium: 4 vCores	Service/UI Version : 4.4.694.2/5.1.4720.7	
Tags (change)	: <a href="#">Click here to add tags</a>		

# New migration project



Project name

MySQL



Source server type \*

MySQL



Target server type \*

Azure Database for MySQL



\*Choose type of activity >

Online data migration

**To successfully use Database Migration Service (DMS) to migrate data, you need to:**

1. Create the target Azure Database for MySQL.
2. Deploy schema, indexes and routines to target database:
  1. Using MySQL Workbench OR
  2. Using mysqldump --no-data



**Create and run activity**

- Add a source (on-premises database).

Migration Wizard		«	»	Add Source Details	□	×
mysql						
<b>1</b>	Select source	>				
<b>2</b>	Select target	>				
<b>3</b>	Select databases	>				
<b>4</b>	Configure migration settings	>				
<b>5</b>	Summary	>				

Source server name  
172.16.0.41

Server port  
3306 ✓

User Name  
root

Password  
\*\*\*\*\*

TLS 1.2 security protocol  
 My server has TLS 1.2 enabled

**i** DMS requires **TLS 1.2 security protocol** enabled to establish an encrypted connection to the source MySQL database.

Follow these steps to enable TLS support:  
[TLS 1.2 support for MySQL](#)

- Select a target.

Migration Wizard		«	»	Target details	□	×
mysql						
<b>1</b>	Select source	✓				
<b>2</b>	Select target	>				
<b>3</b>	Select databases	>				
<b>4</b>	Configure migration settings	>				
<b>5</b>	Summary	>				

Target server name ⓘ  
contoso-mysql.mysql.database.azure.com

User Name  
s2admin@ contoso-mysql

Password  
\*\*\*\*\*

- Select the databases to migrate.

The screenshot shows the 'Migration Wizard' interface with the title 'mysql'. The steps are numbered 1 through 5. Step 1 'Select source' is marked with a green checkmark. Step 2 'Select target' is also marked with a green checkmark. Step 3 'Select databases' has a right-pointing arrow indicating it's the next step. Step 4 'Configure migration settings' and Step 5 'Summary' are shown below with arrows pointing right.

- o Configure advanced settings.

The screenshot shows the 'Migration Wizard' interface with the title 'mysql'. Step 4 'Configure migration settings' is expanded to reveal a configuration pane for the 'osticket' database. Under 'Advanced online migration settings', there is a section for Large Objects (LOB) data. Two radio buttons are present: 'Allow unlimited LOB size' (unchecked) and 'Limit LOB size' (checked). Below this, a text input field shows 'Limit LOB size to (KB):' with the value '32'.

- o Start the replication and resolve any errors.

The screenshot shows the 'on-premises-one' activity details page. At the top, there are buttons for Refresh, Retry, Stop migration, Delete activity, Download report, and a dropdown menu. Below this, the activity status is listed as 'Succeeded'. The table displays the following information:

Source server	Source version	Source databases		
52.191.131.189	MySQL 5.7	1		
Target server	Target version	Type of activity		
osticket.mysql.database.azure.com	Azure Database for MySQL 5.7	Online		
Activity status	Duration			
Succeeded	00:00:32			
Database name	Status	Migration details	Estimated application downtime	Finish Date
OSTICKET	Failed	<a href="#">See error details</a>	---	3/20/2020, 1:25:06 PM

- o Perform the final cutover.

The screenshot shows the 'osticket' activity details page. At the top, there are buttons for Refresh and Start Cutover. The table displays the following migration statistics:

Source database name	Full load completed	Incremental updates	Pending changes
osticket	15	0	0
Target database name	Full load queued	Incremental inserts	Applied changes
osticket	0	0	0
Database status	Full load loading	Incremental deletes	Tables in error state
Running	0	0	0
Migration details	Full load failed		
Ready to cutover	0		

## Complete cutover

X

When you are ready to do the migration cutover, perform the following steps to complete the database migration. Please note that the database is ready for cutover only after the full data load is completed.

1. Stop all the incoming transactions coming to the source database.
2. Wait until all the pending transactions have been applied to the target database. At that time the pending changes counter will set to 0:

Pending changes

0

Confirm

Apply

3. Reconnect your applications to the new Azure target database.

[+ New Activity](#) [Edit Project](#) [Delete project](#) [Refresh](#)

Source server : 52.191.131.189

Target server : contoso-mysql.mysql.database.azure.com

Source version : MySQL 5.7

Target version : Azure Database for MySQL 5.7

^

### Migration Activities (4)

Name	Activity Type	Status	Start Time
on-premises-one	Online data migration	Completed	03/20/2020, 1:24:58 PM
on-premises-one-01	Online data migration	Failed input validation	03/20/2020, 1:24:58 PM
on-premises-one-02	Online data migration	Failed input validation	03/20/2020, 1:24:58 PM
on-premises-one-03	Online data migration	Completed	03/20/2020, 1:24:58 PM

- Reinstate any foreign keys and triggers.
- Modify applications to use the new database.

---

3. Reconnect your applications to the new Azure target database.

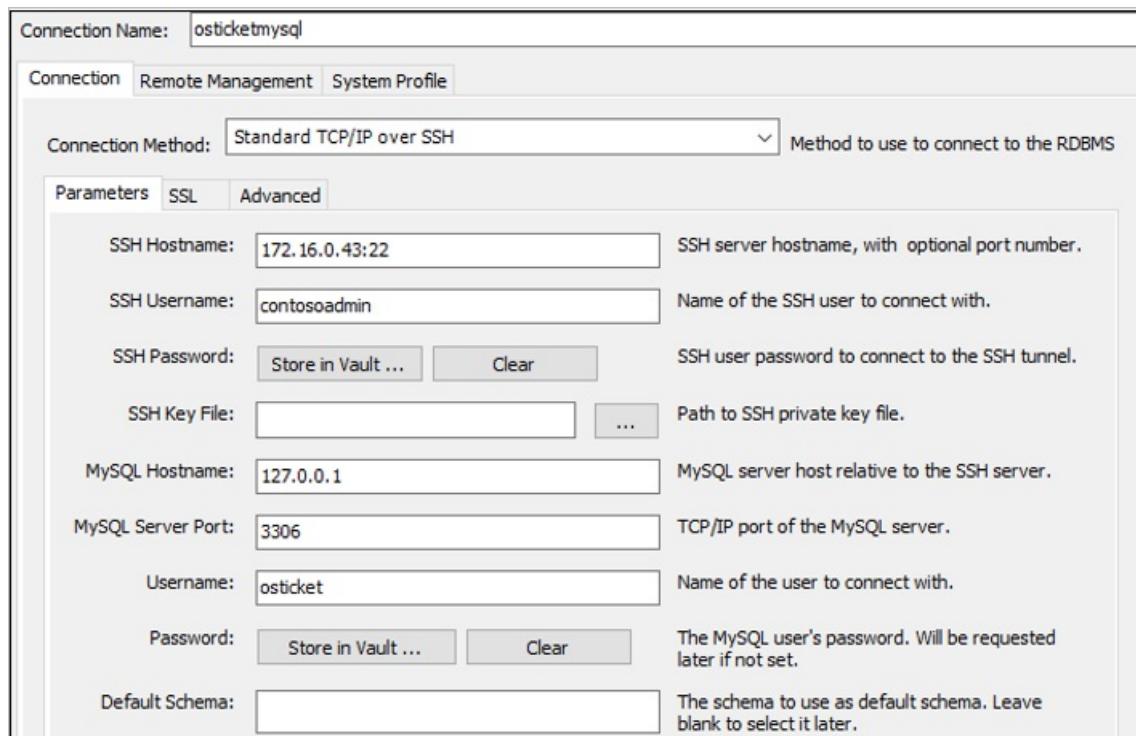
Completed

**Step 6b: Migrate the database (MySQL Workbench)**

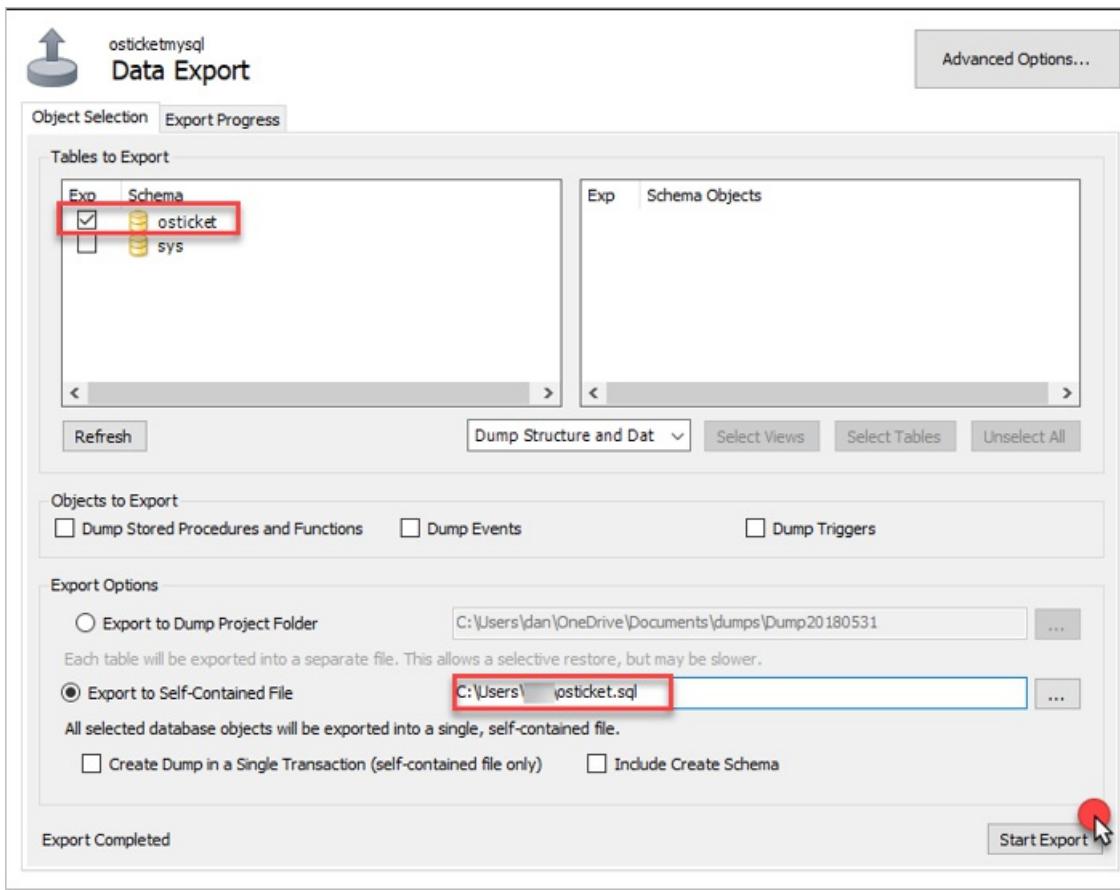
Contoso admins migrate the database by using backup and restore with MySQL tools. They install MySQL Workbench, back up the database from `OSTICKETMYSQL`, and then restore it to Azure Database for MySQL.

**Install MySQL Workbench**

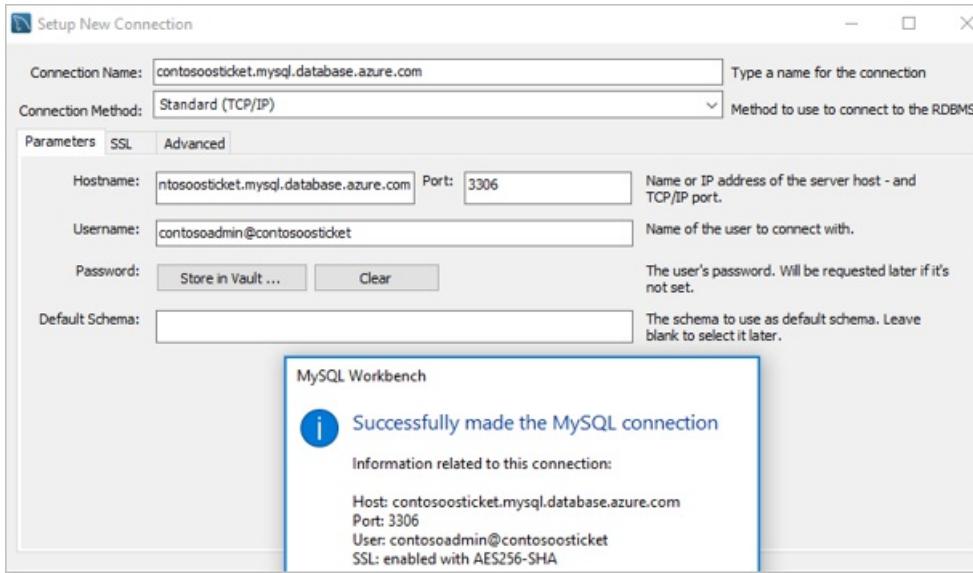
1. Check the [prerequisites, and download MySQL Workbench](#).
2. Install MySQL Workbench for Windows by following the [installation instructions](#).
3. In MySQL Workbench, create a MySQL connection to `OSTICKETMYSQL`.



4. Export the database as `osticket` to a local self-contained file.



5. After the database is backed up locally, create a connection to the Azure Database for MySQL instance.



6. Now, import (restore) the database in the Azure Database for MySQL instance from the self-contained file. A new schema (`osticket`) is created for the instance.

The screenshot shows the 'Data Import' interface for a MySQL database named 'contosoosticket.mysql.database.azure.com'. The 'Import Options' section is visible, with 'Import from Self-Contained File' selected and the file path 'C:\Users\dan\osticket.sql' highlighted with a red box. Below it, the 'Default Schema to be Imported To' section shows 'Default Target Schema: osticket' also highlighted with a red box.

## Connect the VM to the database

As the final step in the migration process, Contoso admins update the connection string of the application to point to the application database running on the `OSTICKETMYSQL` VM.

1. Make an SSH connection to the `OSTICKETWEB` VM by using PuTTY or another SSH client. The VM is private, so connect by using the private IP address.

The dialog title is 'Connect to virtual machine' for 'OSTICKETWEB'. It has tabs for 'RDP' (selected) and 'SSH'. The 'SSH' tab is underlined. Below the tabs, instructions say: 'To connect to your virtual machine via SSH, select an IP address, optionally change the port number, and use one of the following commands:'. There are two input fields: 'IP address' containing 'Private IP address (10.245.32.5)' and 'Port number' containing '22'. At the bottom, there is a 'Login using VM local account' field with the placeholder 'ssh <Login username>@10.245.32.5' and a blue 'Copy' icon.

```
$ ssh contosoadmin@10.245.32.5
The authenticity of host '10.245.32.5 (10.245.32.5)' can't be established.
ECDSA key fingerprint is SHA256:aJNt+VbYqoZb+mrBlCCj5
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '10.245.32.5' (ECDSA) to the list of known hosts.
contosoadmin@10.245.32.5's password:
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.4.0-127-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:     https://landscape.canonical.com
 * Support:        https://ubuntu.com/advantage

136 packages can be updated.
59 updates are security updates.

Last login: [REDACTED] from 172.16.0.200
contosoadmin@osticketweb:~$ |
```

2. Make sure that the `OSTICKETWEB` VM can communicate with the `OSTICKETMYSQL` VM. Currently, the configuration is hardcoded with the on-premises IP address `172.16.0.43`.

Before the update:

```
# Database Options
# -----
# Mysql Login info
define('DBTYPE', 'mysql');
define('DBHOST', '172.16.0.43');
define('DBNAME', 'osticket');
define('DBUSER', 'osticket');
```

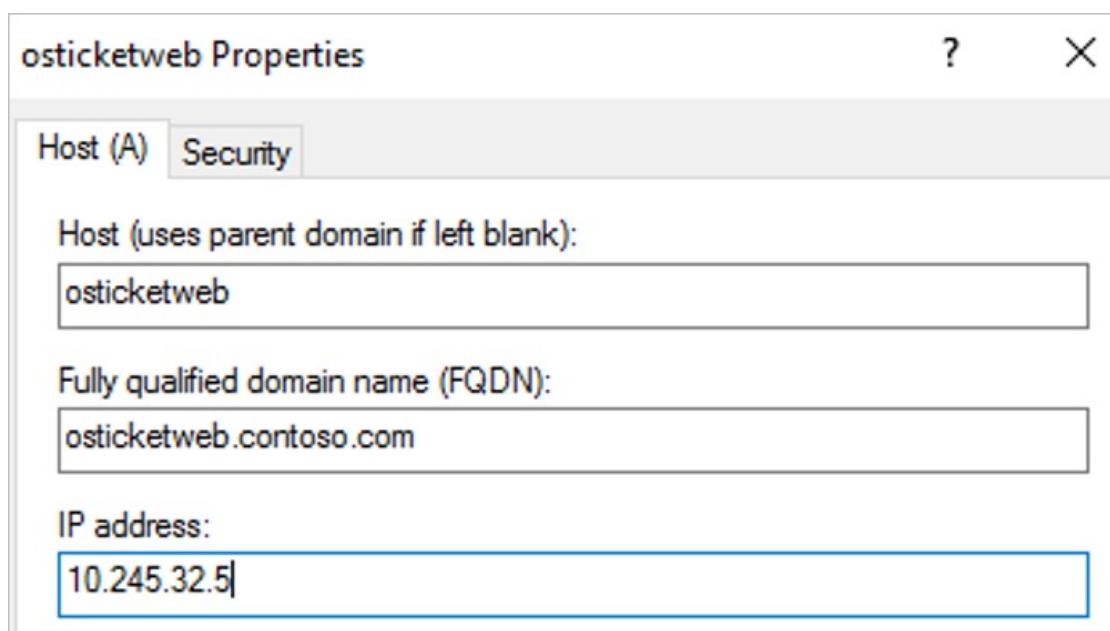
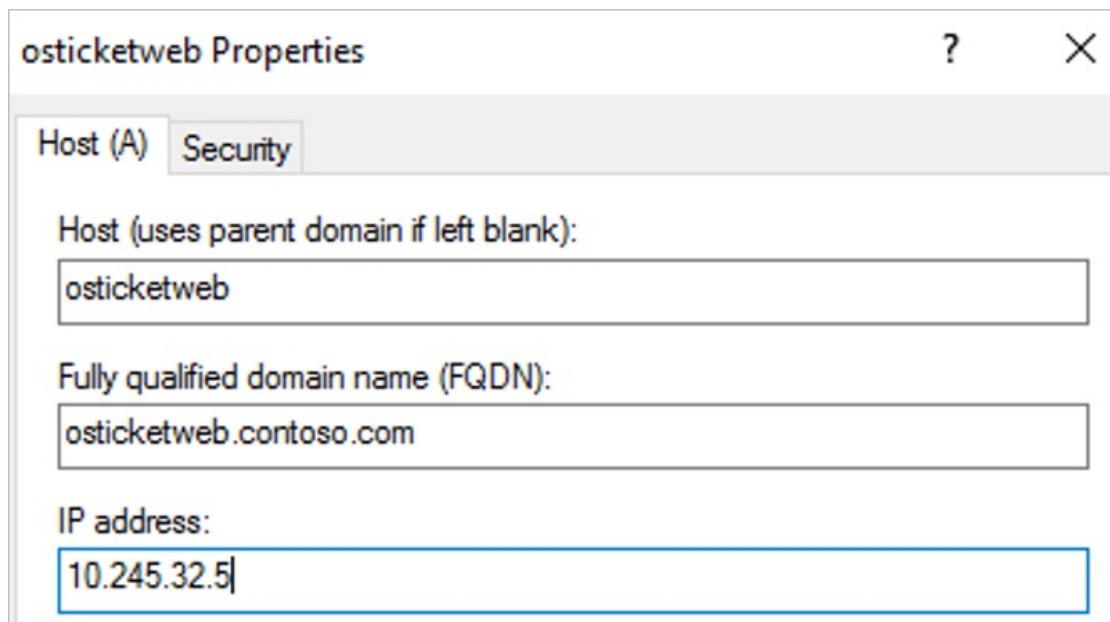
After the update:

```
# Database Options
# -----
# Mysql Login info
define('DBTYPE', 'mysql');
define('DBHOST', 'osticketmysql.contoso.com');
define('DBNAME', 'osticket');
define('DBUSER', 'osticket');
-- INSERT --
```

3. Restart the service with `systemctl restart apache2`.

```
contosoadmin@osticketweb:~$ systemctl restart apache2
==== AUTHENTICATING FOR org.freedesktop.systemd1.manage-units
Authentication is required to restart 'apache2.service'.
Authenticating as: contosoadmin, , , (contosoadmin)
Password:
==== AUTHENTICATION COMPLETE ===
contosoadmin@osticketweb:~$
```

4. Finally, update the DNS records for `OSTICKETWEB` and `OSTICKETMYSQL` on one of the Contoso domain controllers.



#### Need more help?

- Learn about how to [run a test migration](#).
- Learn about how to [migrate VMs to Azure](#).

## Review the deployment

With the application now running, Contoso needs to fully operationalize and secure its new infrastructure.

## Clean up after migration

With migration complete, the osTicket application tiers are running on Azure VMs.

Now, Contoso needs to do the following tasks:

- Remove the VMware VMs from the vCenter inventory.
- Remove the on-premises VMs from local backup jobs.
- Update internal documentation to show new locations and IP addresses.
- Review any resources that interact with the on-premises VMs. Update any relevant settings or documentation to reflect the new configuration.

- Contoso used Azure Migrate with dependency mapping to assess the [OSTICKETWEB](#) VM for migration.

## Security

The Contoso security team reviews the VM and database to determine any security issues:

- They review the network security groups (NSGs) for the VM to control access. NSGs are used to ensure that only traffic allowed to the application can pass.
- They consider securing the data on the VM disks by using Azure Disk Encryption and Azure Key Vault.
- Communication between the VM and database instance isn't configured for SSL. They'll need to configure SSL to ensure that database traffic can't be hacked.

For more information, see [Security best practices for IaaS workloads in Azure](#).

## Business continuity and disaster recovery

For business continuity and disaster recovery, Contoso takes the following actions:

- Keep data safe.** Contoso backs up the data on the application VM by using [Azure VM backup](#). The company doesn't need to configure backup for the database. Azure Database for MySQL automatically creates and stores server backups. Contoso selected to use geo-redundancy for the database so that it's resilient and production ready.
- Keep applications up and running.** Contoso replicates the application VMs in Azure to a secondary region by using Site Recovery. For more information, see [Quickstart: Set up disaster recovery to a secondary Azure region for an Azure VM](#).

## Licensing and cost optimization

- After deploying resources, Contoso assigns Azure tags as defined during the [Azure infrastructure](#) deployment.
- There are no licensing issues for the Contoso Ubuntu servers.
- Contoso will use [Azure Cost Management and Billing](#) to ensure the company stays within budgets established by the IT leadership.

# Rehost an on-premises dev/test environment on Azure Virtual Machines via Azure Migrate

11/9/2020 • 14 minutes to read • [Edit Online](#)

This article demonstrates how the fictional company Contoso rehosts its dev/test environment for two applications running on VMware virtual machines (VMs) by migrating to Azure Virtual Machines.

The [SmartHotel360](#) and [osTicket](#) applications used in this example are open source. You can download them for your own testing purposes.

## Migration options

Contoso has several options available for moving dev/test environments to Azure:

MIGRATION OPTIONS	OUTCOME
Azure Migrate	<p><a href="#">Assess and migrate</a> on-premises VMs.</p> <p>Run dev/test servers by using Azure infrastructure as a service (IaaS).</p> <p>Manage VMs with <a href="#">Azure Resource Manager</a>.</p>
Azure DevTest Labs	<p>Quickly provision development and test environments.</p> <p>Minimize waste with quotas and policies.</p> <p>Set automated shutdowns to minimize costs.</p> <p>Build Windows and Linux environments.</p>

### NOTE

Read how Contoso moved its [dev/test environment to Azure](#) by using DevTest Labs.

## Business drivers

The development leadership team has outlined what it wants to achieve with this migration. It aims to quickly move dev/test capabilities out of an on-premises datacenter and no longer purchase hardware to develop software. It also seeks to empower developers to create and run their environments without involvement from IT.

### NOTE

Contoso will use the [Pay-As-You-Go Dev/Test subscription offer](#) for its environments. Each active Visual Studio subscriber on the team can use the Microsoft software included with the subscription virtual machines for dev/test at no extra charge. Contoso will just pay the Linux rate for VMs that it runs. That includes VMs with SQL Server, SharePoint Server, or other software that's normally billed at a higher rate.

## Migration goals

The Contoso development team has pinned down goals for this migration. These goals are used to determine the best migration method:

- Contoso wants to quickly move out of its on-premises dev/test environments.
- After migration, Contoso's dev/test environment in Azure should have enhanced capabilities over the current system in VMware.
- The operations model will move from IT provisioned to DevOps with self-service provisioning.

## Solution design

After pinning down goals and requirements, Contoso designs and reviews a deployment solution and identifies the migration process. The process includes the Azure services that Contoso will use for the migration.

### Current application

- The dev/test VMs for the two applications are running on VMs (`WEBVMDEV`, `SQLVMDEV`, `OSTICKETWEBDEV`, `OSTICKETMYSQLDEV`). These VMs are used for development before code is promoted to the production VMs.
- The VMs are located on VMware ESXi host `contosohost1.contoso.com` (version 6.5).
- The VMware environment is managed by vCenter Server 6.5 (`vcenter.contoso.com`), running on a VM.
- Contoso has an on-premises datacenter (`contoso-datacenter`) with an on-premises domain controller (`contosodc1`).

### Proposed architecture

- Because the VMs are used for dev/test, they'll reside in the `ContosoDevRG` resource group in Azure.
- The VMs will be migrated to the primary Azure region (`East US 2`) and placed in the development virtual network (`VNET-DEV-EUS2`).
- The web front-end VMs will reside in the front-end subnet (`DEV-FE-EUS2`) in the development network.
- The database VM will reside in the database subnet (`DEV-DB-EUS2`) in the development network.
- The on-premises VMs in the Contoso datacenter will be decommissioned after the migration is done.

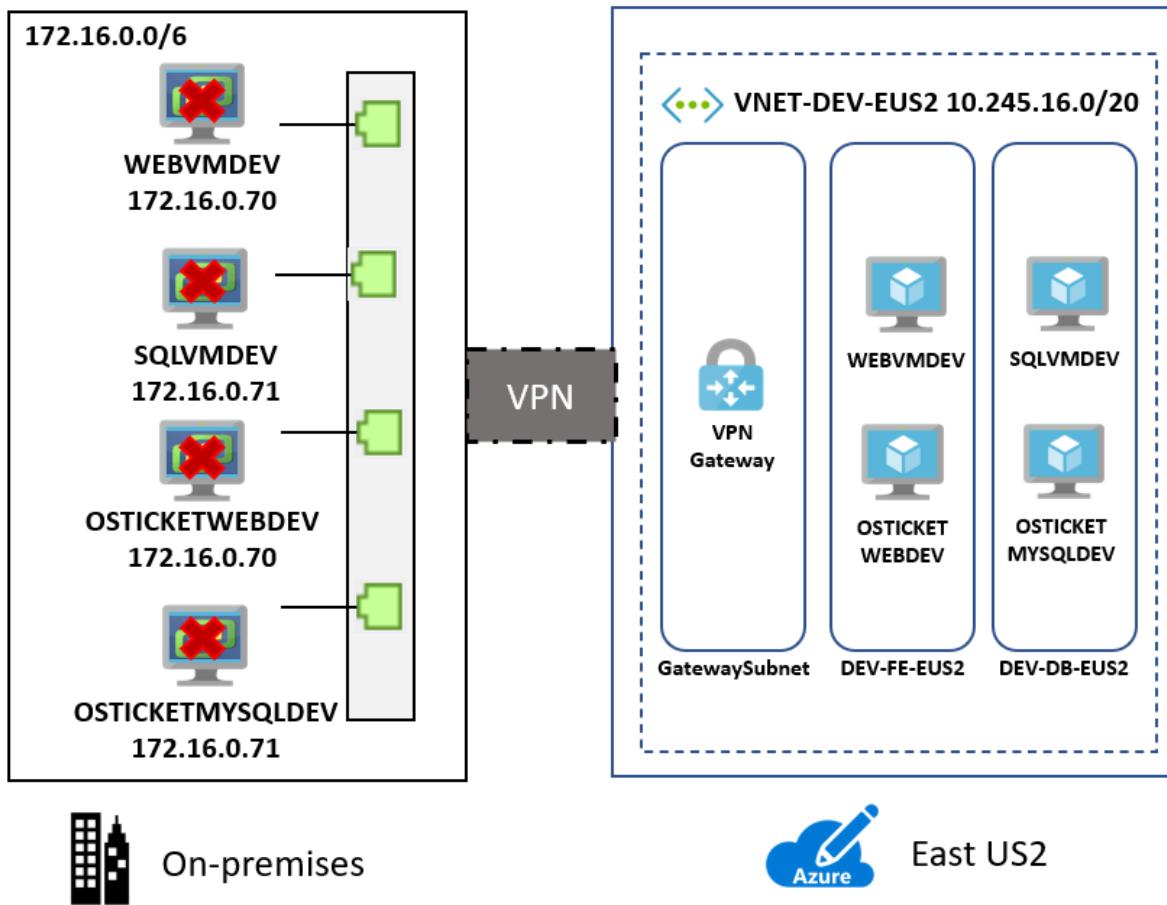


Figure 1: Proposed architecture.

### Database considerations

To support ongoing development, Contoso has decided to continue using existing VMs and migrate them to Azure. In the future, Contoso will pursue the use of platform as a service (PaaS) services such as [Azure SQL Database](#) and [Azure Database for MySQL](#).

- Database VMs will be migrated as is without changes.
- With the use of the Azure Dev/Test subscription offer, the computers running Windows Server and SQL Server will not incur licensing fees. Avoiding fees will keep the compute costs to a minimum.
- In the future, Contoso will look to integrate its development with PaaS services.

### Solution review

Contoso evaluates the proposed design by putting together a list of pros and cons.

CONSIDERATION	DETAILS
---------------	---------

CONSIDERATION	DETAILS
Pros	<p>All of the development VMs will be moved to Azure without changes, making the migration simple.</p> <p>Because Contoso is using a lift-and-shift approach for both sets of VMs, special configuration or migration tools aren't needed for the application database.</p> <p>Contoso can take advantage of its investment in the Azure Dev/Test subscription to save on licensing fees.</p> <p>Contoso will retain full control of the application VMs in Azure.</p> <p>Developers will be provided with rights to the subscription, which empowers them to create new resources without waiting for IT to respond to their requests.</p>
Cons	<p>The migration will only move the VMs, not yet moving to PaaS services for their development. This means that Contoso will need have to start supporting the operations of its VMs, including security patches. This was maintained by IT in the past, so Contoso will need to find a solution for this new operational task.</p> <p>The cloud-based solution empowers the developers and doesn't have safeguards for overprovisioning systems. Developers will be able to instantly provision their systems, but they might create resources that cost money and aren't included in the budget.</p>

#### NOTE

Contoso could address the cons in its list by using [Dev/Test Labs](#).

#### Migration process

Contoso will migrate its development front end and database to Azure VMs by using the agentless method in the Azure Migrate: Server Migration tool.

- Contoso prepares and sets up Azure components for Azure Migrate: Server Migration, and prepares the on-premises VMware infrastructure.
- The **Azure infrastructure** is in place, so Contoso just needs to configure the replication of the VMs through the Azure Migrate: Server Migration tool.
- With everything prepared, Contoso can start replicating the VMs.
- After replication is enabled and working, Contoso migrates the VMs by testing the migration and if successful, failing it over to Azure.
- After the development VMs are up and running in Azure, Contoso will reconfigure its development workstations to point at the VMs now running in Azure.

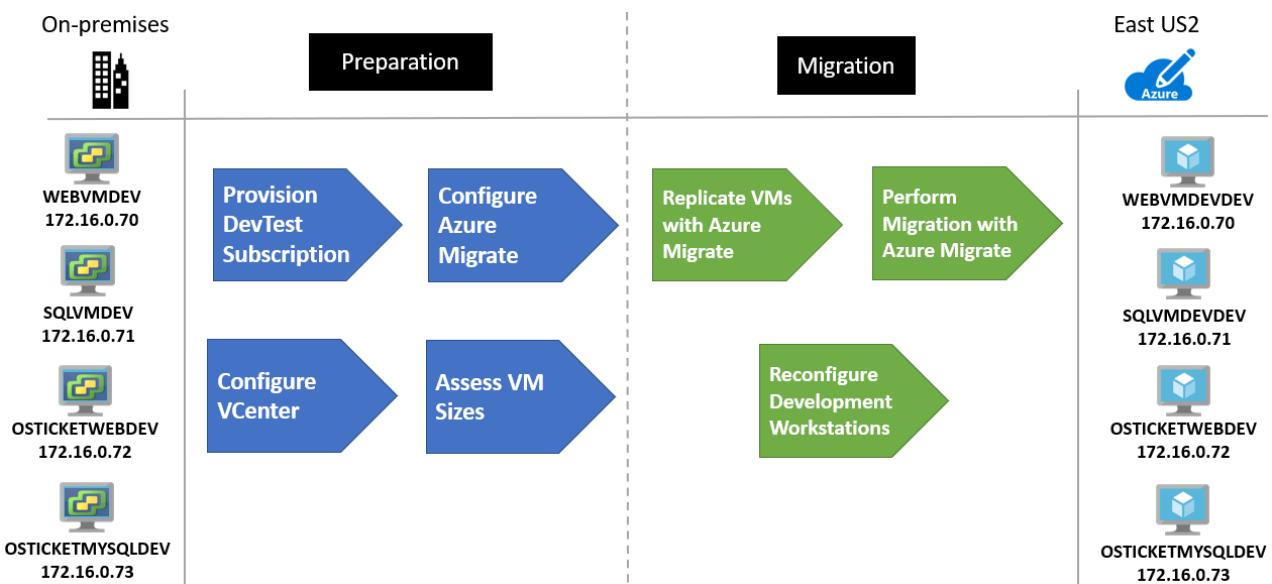


Figure 2: An overview of the migration process.

## Azure services

Service	Description	Cost
Azure Migrate: Server Migration	The service orchestrates and manages migrating on-premises applications and workloads and AWS or GCP VM instances.	During replication to Azure, Azure Storage charges are incurred. Azure VMs are created and incur charges when the migration occurs and the VMs are running in Azure. Learn more about <a href="#">charges and pricing</a> .

## Prerequisites

This is what Contoso needs to run this scenario:

Requirements	Details
Azure Dev/Test subscription	<p>Contoso creates an <a href="#">Azure Dev/Test subscription</a> to take advantage of reducing costs up to 80 percent.</p> <p>If you don't have an Azure subscription, create a <a href="#">free account</a>.</p> <p>If you create a free account, you're the admin of your subscription, and you can perform all actions.</p> <p>If you use an existing subscription but you're not the admin, work with the admin to assign you Owner or Contributor permissions.</p> <p>If you need more granular permissions, see <a href="#">Manage Site Recovery access with role-based access control (RBAC)</a>.</p>
Azure infrastructure	<p>Learn how Contoso <a href="#">set up an Azure infrastructure</a>.</p> <p>Learn more about specific <a href="#">prerequisites</a> for Azure Migrate: Server Migration.</p>

Requirements	Details
On-premises servers	<p>On-premises vCenter servers should be running version 5.5, 6.0, 6.5, or 6.7.</p> <p>ESXi hosts should run version 5.5, 6.0, 6.5, or 6.7.</p> <p>One or more VMware VMs should be running on the ESXi host.</p>

## Scenario steps

Here's how Contoso admins will run the migration:

- **Step 1: Prepare Azure for Azure Migrate: Server Migration.** They add the server migration tool to their Azure Migrate project.
- **Step 2: Prepare on-premises VMware for Azure Migrate: Server Migration.** They prepare accounts for VM discovery and prepare to connect to Azure VMs after migration.
- **Step 3: Replicate VMs.** They set up replication and start replicating VMs to Azure Storage.
- **Step 4: Migrate the VMs with Azure Migrate: Server Migration.** They run a test migration to make sure everything's working and then run a full migration to move the VMs to Azure.

## Step 1: Prepare Azure for the Azure Migrate: Server Migration tool

Contoso needs to migrate the VMs to a virtual network where the Azure VMs will reside when they're created, provisioned, and configured through the Azure Migrate: Server Migration tool.

1. Set up a network: Contoso already set up a network that can be for Azure Migrate: Server Migration when it [deployed the Azure infrastructure](#).
  - The VMs to be migrated are used for development. They will migrate to the Azure development virtual network (`VNET-DEV-EUS2`) in the primary `East US 2` region.
  - Both VMs will be placed in the `ContosoDevRG` resource group, which is used for development resources.
  - The application front-end VMs (`WEBVMDEV` and `OSTICKETWEBDEV`) will migrate to the front-end subnet (`DEV-FE-EUS2`), in the development virtual network.
  - The application database VM (`SQLVMDEV` and `OSTICKETMYSQLDEV`) will migrate to the database subnet (`DEV-DB-EUS2`), in the development virtual network.
2. Provision the Azure Migrate: Server Migration tool.
  - a. From Azure Migrate, download the .OVA image and import it into VMware.

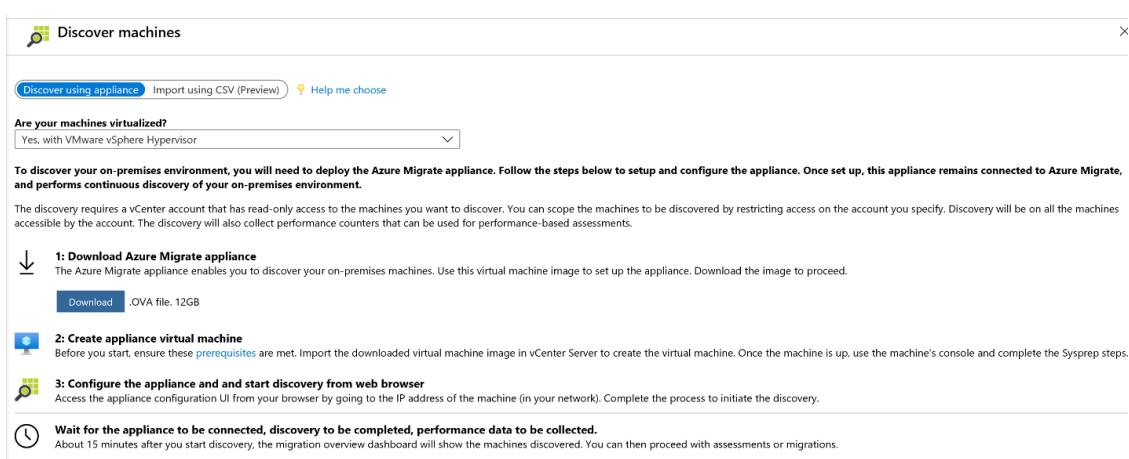


Figure 3: Download the .OVA file.

b. Start the imported image and configure the tool, including the following steps:

- Set up the prerequisites.

The screenshot shows the 'Set up discovery for Azure Migrate' wizard. The current step is 'Set up prerequisites'. A sub-step titled 'Verify and set up appliance prerequisites' is displayed. It contains several checklist items:

- Accept license terms [View terms of use](#)
- Use of the Azure Migrate Appliance (the "software") is licensed to you as part of your or your company's subscription for the Azure Migrate Service (the "service"). Your use of the software is governed by the agreement under which you or your company obtained the service (see [Azure Legal Information](#)). Microsoft assumes no responsibility or liability whatsoever for any non-Microsoft product made available to you through your use of the service or software. Customer is solely responsible for any non-Microsoft product that it installs or uses with the service or software and acknowledges that use shall be governed by the separate agreement(s) between Customer and the publisher of the non-Microsoft product. See [TPN](#) for third-party components included in the software.
- Check connectivity to the Internet [Set up proxy](#)
- Check time is in sync with the Internet time server
- Check if latest Azure Migrate updates are installed
- Install VMware vSphere Virtual Disk Development Kit

A 'Continue' button is located at the bottom right of the checklist area. Below the checklist, there is another section titled 'Register with Azure Migrate' with the sub-instruction 'Specify your Microsoft Azure account details'.

Figure 4: Setting up the prerequisites.

- Point the tool to the Azure subscription.

## Azure Migrate Appliance

### Set up discovery for Azure Migrate

Azure Migrate appliance helps you discover, assess and migrate your VMware virtual machines. Complete the following steps to initiate discovery. [Learn more](#) about Azure Migrate discovery capabilities.

The screenshot shows the 'Register with Azure Migrate' step of the setup process. It includes a descriptive text about choosing a subscription and resource group, a 'Logged in as' dropdown, a 'Logout' button, and fields for 'Subscription', 'Migrate project', 'Enter Appliance Name', and a 'Register' button. A 'Continue' button is located at the bottom right of the main panel.

Figure 5: The Azure subscription.

- Set the VMware vCenter credentials.

The screenshot shows the 'Specify vCenter Server' step. It provides details for discovering machines and choosing VM credentials for dependencies. The main panel shows fields for 'vCenter Server name/IP' (192.168.102.91), 'Port' (443), 'User name' (administrator@), 'Password' (redacted), and a 'Validate connection' button which displays a success message: 'Successfully connected to vCenter Server'. A note at the bottom explains metadata discovery.

Figure 6: Setting the VMware vCenter credentials.

- Add any Windows-based credentials for discovery.

Discover applications and dependencies on VMs

Provide VM credentials for discovery of applications and for dependency analysis on the machines. Ensure 'Guest Operations' privileges are enabled for these VMs. [Learn more](#) about permissions.

The credentials will be saved on the appliance in an encrypted format. The discovery of applications and dependencies is done remotely without the installation of any agent or script on VMs.

[Add credentials](#)

Skip addition of VM credentials. You will not be able to discover applications and dependencies.

Added credentials

OS Type	Friendly Name	Action
Windows	basic	Edit
Linux	basic-linux	Edit

[Save and start discovery](#)

Figure 7: Adding Windows-based credentials for discovery.

- When you complete the configuration, the tool will take some time to enumerate all the VMs. You'll see them populate the Azure Migrate tool in Azure when this process finishes.

#### Need more help?

Learn how to [set up the Azure Migrate: Server Migration tool](#).

#### Prepare on-premises VMs

After migration, Contoso wants to connect to the Azure VMs and allow Azure to manage the VMs. To do this, Contoso admins do the following before migration:

- For access over the internet, they:
  - Enable RDP or SSH on the on-premises VM before migration.
  - Ensure that TCP and UDP rules are added for the `Public` profile.
  - Check that RDP or SSH is allowed in the operating system firewall.
  - Install SSH via the following command: `sudo apt-get ssh install -y`.
- For access over Site-to-Site VPN, they:
  - Enable RDP or SSH on the on-premises VM before migration.
  - Check that RDP or SSH is allowed in the operating system firewall.
  - For Windows, set the operating system's SAN policy on the on-premises VM to `onlineAll`.
- Install the [Azure Windows agent](#) and the [Azure Linux agent](#).

For Windows, there shouldn't be Windows updates pending on the VM when you're triggering a migration. If there are, the admins won't be able to log in to the VM until the updates finish. After migration, the admins can check **Boot diagnostics** to view a screenshot of the VM. If this doesn't work, they should verify that the VM is running and review [troubleshooting tips](#).

#### Need more help?

Learn how to [prepare VMs for migration](#).

## Step 3: Replicate the on-premises VMs

Before Contoso admins can run a migration to Azure, they need to set up and enable replication. With discovery completed, they can begin replicating VMware VMs to Azure.

1. In the Azure Migrate project, go to **Servers > Azure Migrate: Server Migration**. Then select **Replicate**.

The screenshot shows the Azure Migrate - Servers dashboard. On the left, there's a navigation menu with options like Overview, Migration goals (Servers selected), Databases, Data Box, Manage, Discovered items, Support + troubleshooting, and New support request. The main area has two sections: **Assessment tools** and **Migration tools**. The Assessment tools section contains a summary of discovered servers (442), groups (2), assessments (2), and notifications (0). It also includes a callout for starting migration or refining application grouping. The Migration tools section shows the Azure Migrate: Server Migration interface with tabs for Discover, Replicate (highlighted with a red box), Migrate, and Overview. Below these tabs, it shows 442 discovered servers.

Figure 8: Replicating VMs.

2. In **Replicate > Source settings > Are your machines virtualized?**, select Yes, with VMware vSphere.
3. In **On-premises appliance**, select the name of the Azure Migrate appliance that you set up, and then select OK.

The screenshot shows the Replicate dialog box. At the top, it says "Replicate". Below that is a navigation bar with tabs: Source settings (selected), Virtual machines, Target settings, Compute, Disks, and Review + Start replication. The Source settings tab contains a note about replicating servers. Under "Are your machines virtualized?", there's a dropdown menu with "Yes, with VMware vSphere" selected. Under "On-premises appliance", there's a dropdown menu with "<onprem-name>" selected.

Figure 9: The source settings.

4. In **Virtual machines**, select the machines that you want to replicate.
  - If you've run an assessment for the VMs, you can apply VM sizing and disk type (premium or standard) recommendations from the assessment results. To do this, in **Import migration settings from an Azure Migrate assessment?**, select the **Yes** option.
  - If you didn't run an assessment or you don't want to use the assessment settings, select the **No** option.
  - If you selected to use the assessment, select the VM group and assessment name.

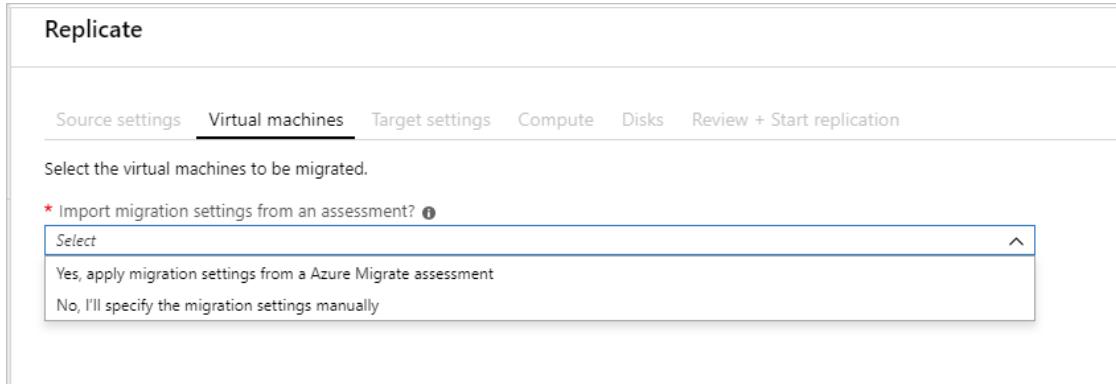


Figure 10: How to set up the prerequisites.

5. In **Virtual machines**, search for VMs as needed and check each VM you want to migrate. Then select **Next: Target settings**.
6. In **Target settings**, select the subscription and target region to which you'll migrate. Then specify the resource group in which the Azure VMs will reside after migration. In **Virtual Network**, select the virtual network or subnet to which the Azure VMs will be joined after migration.
7. In **Azure Hybrid Benefit**, select **No** if you don't want to apply Azure Hybrid Benefit. Then select **Next**. Select **Yes** if you have Windows Server machines that are covered with active Software Assurance or Windows Server subscriptions and you want to apply the benefit to the machines you're migrating. Then select **Next**.

**NOTE**

In the case of Contoso, the admins will select **No** to Azure Hybrid Benefit because this is an Azure Dev/Test subscription. This means they'll pay for the compute only. [Azure Hybrid Benefit](#) should be used only for production systems that have Software Assurance benefits.

8. In **Compute**, review the VM name, size, OS disk type, and availability set. VMs must conform with [Azure requirements](#).
  - **VM size:** If you're using assessment recommendations, this drop-down list contains the recommended size. Otherwise, Azure Migrate selects a size based on the closest match in the Azure subscription. You can choose a manual size instead in [Azure VM size](#).
  - **OS disk:** Specify the OS (boot) disk for the VM. The OS disk has the operating system bootloader and installer.
  - **Availability set:** If the VM should be in an Azure availability set after migration, then specify the set. The set must be in the target resource group that you specify for the migration.
9. In **Disks**, specify whether the VM disks should be replicated to Azure and select the disk type (standard

SSD/HDD or premium managed disks) in Azure. Then select **Next**. You can exclude disks from replication. If you do, they won't be present on the Azure VM after migration.

10. In **Review and start replication**, review the settings and select **Replicate** to start the initial replication for the servers.

**NOTE**

You can update replication settings at any time before replication starts in **Manage > Replicating machines**. Settings can't be changed after replication starts.

## Step 4: Migrate the VMs

Contoso admins run a quick test migration and then a full migration to migrate the VMs.

### Run a test migration

1. In **Migration goals > Servers > Azure Migrate: Server Migration**, select **Test migrated servers**.

The screenshot shows the 'Migration tools' interface for 'Azure Migrate: Server Migration'. At the top, there are four navigation links: 'Discover', 'Replicate', 'Migrate', and 'Overview'. Below these are four status cards:

- Discovered servers:** 442
- Replicating servers:** 6
- Test migrated servers:** 1 (This card is highlighted with a red box)
- Migrated servers:** 1

At the bottom, there is a note: **Next step:** You can start migrating the replicating servers to Azure.

Figure 11: Testing migrated servers.

2. Select and hold (or right-click) the VM to test, and then select **Test migrate**.

The screenshot shows the 'Azure Migrate - Servers' blade. On the left, there's a sidebar with 'Getting started' and 'Replicating machines' selected. The main area shows a table for 'Replicating machines':

NAME	STATUS	HEALTH	MIGRATION PHASE	LAST SYNC	TEST MIGRATION STATUS
Contoso-Win2K8R2SP1	Delta sync	Healthy	Test migration pending	2/17/2019, 12:00:43 AM	Never performed

A context menu is open over the first row, with the 'Test migrate' option highlighted by a red box. Other options in the menu include 'Pin to dashboard', 'Clean up test migration', and 'Migrate'.

Figure 12: Testing the migration.

3. In **Test Migration**, select the virtual network in which the Azure VM will be located after the migration. We recommend that you use a nonproduction virtual network.

4. The **Test migration** job starts. Monitor the job in the portal notifications.
5. After the migration finishes, view the migrated Azure VM in **Virtual Machines** in the Azure portal. The machine name has a **-Test** suffix.
6. After the test is done, select and hold (or right-click) the Azure VM in **Replicating machines**, and then select **Clean up test migration**.

NAME	STATUS	HEALTH	MIGRATION PHASE	LAST SYNC	TEST MIGRATION STATUS
Contoso-Win2K8R2SP1	Delta sync	Healthy	Test clean up pending	2/17/2019, 12:00:43 AM	<a href="#">Pin to dashboard</a> <a href="#">Test migrate</a> <b>Clean up test migration</b> (highlighted) <a href="#">Migrate</a> <a href="#">Error Details</a>

Figure 13: Cleaning up the test migration.

## Migrate the VMs

Now Contoso admins run a full migration.

1. In the Azure Migrate project, select **Servers > Azure Migrate: Server Migration > Replicating servers**.

**Migration tools**

**Azure Migrate: Server Migration**

- + Discover
- Replicate
- Migrate
- Overview**

Discovered servers	58
Replicating servers	1
Test migrated servers	0
Migrated servers	0

**Next step:** You can start migrating the replicating servers to Azure

Figure 14: Replicating servers.

2. In **Replicating machines**, select and hold (or right-click) the VM, and then select **Migrate**.
3. In **Migrate > Shut down virtual machines and perform a planned migration with no data loss**, select **Yes** > **OK**. By default, Azure Migrate shuts down the on-premises VM and runs an on-demand replication to synchronize any VM changes that occurred since the last replication occurred. This ensures no data loss. If you don't want to shut down the VM, select **No**.
4. A migration job starts for the VM. Track the job in Azure notifications.
5. After the job finishes, you can view and manage the VM from the **Virtual Machines** page.

**Need more help?**

Learn how to [run a test migration](#) and how to [migrate VMs to Azure](#).

## Clean up after migration

The development VMs for both the SmartHotel360 and osTicket applications start running on Azure VMs when the migration is complete.

Now, Contoso needs to complete these cleanup steps:

- After the migration is complete, stop replication.
- Remove the `WEBVMDEV`, `SQLVMDEV`, `OSTICKETWEBDEV`, and `OSTICKETMYSQLDEV` VMs from the vCenter inventory.
- Remove all the VMs from local backup jobs.
- Update internal documentation to show the new location and IP addresses for the VMs.
- Review any resources that interact with the VMs, and update any relevant settings or documentation to reflect the new configuration.

## Review the deployment

With the application now running, Contoso now needs to fully operationalize and secure it in Azure.

### Security

The Contoso security team reviews the Azure VMs to determine any security issues. To control access, the team reviews the network security groups (NSGs) for the VMs. NSGs are used to ensure that only traffic allowed to the application can reach it. The team also considers securing the data on the disk by using Azure Disk Encryption and Azure Key Vault.

For more information, see [Security best practices for IaaS workloads in Azure](#).

## Business continuity and disaster recovery

For business continuity and disaster recovery, Contoso takes the following action: keep data safe. Contoso backs up the data on the VMs by using the Azure Backup service. For more information, see [An overview of Azure VM backup](#).

### Licensing and cost optimization

Contoso will ensure that all development Azure resources are created through this dev/test subscription to save 80 percent. The admins will enable [Azure Cost Management + Billing](#) to help monitor and manage the Azure resources.

## Conclusion

In this article, Contoso rehosted the development VMs used for its SmartHotel360 and osTicket applications in Azure. The admins migrated the application VMs to Azure VMs by using the Azure Migrate: Server Migration tool.

# Migrate a dev/test environment to Azure DevTest Labs

11/9/2020 • 11 minutes to read • [Edit Online](#)

This article demonstrates how the fictional company Contoso migrates its dev/test environment to Azure DevTest Labs.

## Migration options

Contoso has several options available when moving its dev/test environment to Azure.

MIGRATION OPTIONS	OUTCOME
Azure Migrate	<p>Assess and <a href="#">migrate</a> on-premises VMs.</p> <p>Run dev/test servers by using Azure infrastructure as a service (IaaS).</p> <p>Manage VMs with <a href="#">Azure Resource Manager</a>.</p>
DevTest Labs	<p>Quickly provision development and test environments.</p> <p>Minimize waste with quotas and policies.</p> <p>Set automated shutdowns to minimize costs.</p> <p>Build Windows and Linux environments.</p>

### NOTE

This article focuses on using DevTest Labs to move an on-premises dev/test environment to Azure. Read how [Contoso moved dev/test to Azure IaaS](#) via Azure Migrate.

## Business drivers

The development leadership team has outlined what it wants to achieve with this migration:

- Empower developers with access to DevOps tools and self-service environments.
- Give access to DevOps tools for continuous integration/continuous delivery (CI/CD) pipelines and cloud-native tools for dev/test, such as AI, machine learning, and serverless.
- Ensure governance and compliance in dev/test environments.
- Save costs by moving all dev/test environments out of the datacenter and no longer purchase hardware to develop software.

**NOTE**

Contoso will use the [Pay-As-You-Go Dev/Test subscription offer](#) for its environments. Each active Visual Studio subscriber on the team can use the Microsoft software included with the subscription on Azure Virtual Machines for dev/test at no extra charge. Contoso will just pay the Linux rate for VMs that it runs. That includes VMs with SQL Server, SharePoint Server, or other software that's normally billed at a higher rate.

**NOTE**

Azure customers with an Enterprise Agreement can also benefit from the [Azure Dev/Test subscription offer](#). To learn more, review the video for [enabling and creating EA Dev/Test subscriptions through the EA portal](#).

## Migration goals

The Contoso development team has pinned down goals for this migration. These goals are used to determine the best migration method:

- Quickly provision development and test environments. It should take minutes, not months, to build the infrastructure that a developer needs to write or test software.
- After migration, Contoso's dev/test environment in Azure should have enhanced capabilities over the current system on-premises.
- The operations model will move from IT-provisioned VMs to DevOps with self-service provisioning.
- Contoso wants to quickly move out of its on-premises dev/test environments.
- All developers will connect to dev/test environments remotely and securely.

## Solution design

After pinning down goals and requirements, Contoso designs and reviews a deployment solution. The solution includes the Azure services that it will use for dev/test.

### Current architecture

- The dev/test VMs for Contoso's applications are running on VMware in the on-premises datacenter.
- These VMs are used for development and testing before code is promoted to the production VMs.
- Developers maintain their own workstations, but they need new solutions for connecting remotely from home offices.

### Proposed architecture

- Contoso will use an [Azure Dev/Test subscription](#) to reduce costs for Azure resources. This subscription offers significant savings, including VMs that don't incur licensing fees for Microsoft software.
- Contoso will use DevTest Labs for managing the environments. New VMs will be created in DevTest Labs to support the move to new tools for development and testing in the cloud.
- The on-premises dev/test VMs in the Contoso datacenter will be decommissioned after the migration is done.
- Developers and testers will have access to Windows Virtual Desktop for their workstations.

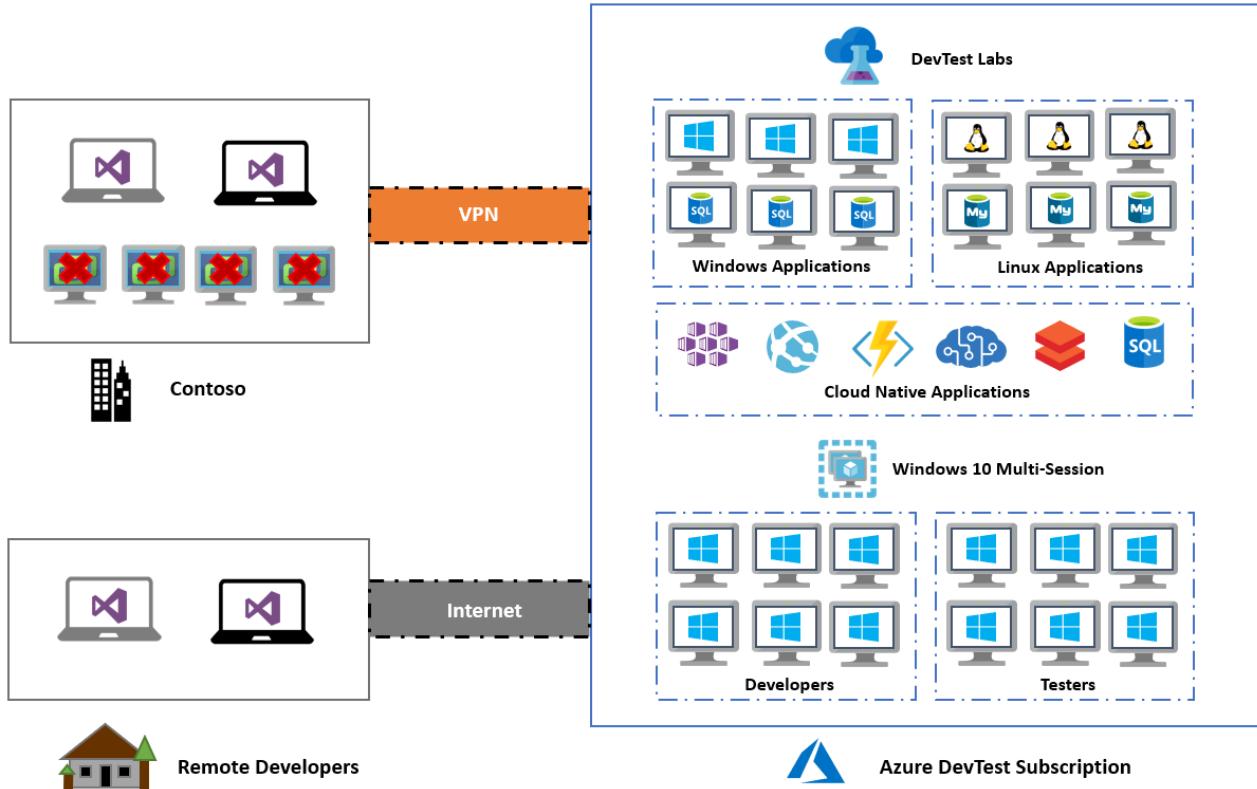


Figure 1: Scenario architecture.

### Database considerations

To support ongoing development, Contoso has decided to continue using databases running on VMs. But the current VMs will be replaced with new ones running in DevTest Labs. In the future, Contoso will pursue the use of platform as a service (PaaS) services such as [Azure SQL Database](#) and [Azure Database for MySQL](#).

Current VMware database VMs will be decommissioned and replaced with Azure VMs in DevTest Labs. The existing databases will be migrated with simple backups and restores. Using the Azure Dev/Test subscription offer won't incur licensing fees for the Windows Server and SQL Server instances, minimizing compute costs.

### Solution review

Contoso evaluates the proposed design by putting together a list of pros and cons.

CONSIDERATION	DETAILS
<b>Pros</b>	<ul style="list-style-type: none"> <li>All of the current development VMs (application and database) will be replaced by new VMs running in DevTest Labs. This means they can take advantage of the features of a purpose-built cloud development environment.</li> <li>Contoso can take advantage of its investment in the Azure Dev/Test subscription to save on licensing fees.</li> <li>Contoso will retain full control of the application VMs in Azure.</li> <li>Developers will be provided with rights to the subscription, which empowers them to create new resources without waiting for IT to respond to their requests.</li> </ul>

CONSIDERATION	DETAILS
Cons	<p>The migration will only move development to the cloud. Developers won't be using PaaS services in their development because they're still using VMs. This means that Contoso will need to start supporting the operations of its VMs, including security patches. IT maintained VMs in the past, and Contoso will need to find a solution for this new operational task.</p> <p>Contoso will have to build new application and database VMs, automating the process. This means it can take advantage of building VMs in the cloud and tools provided by DevTest Labs. So this is a positive outcome even with a con on the list.</p>

## Migration process

Contoso will migrate its development application and database VMs to new Azure VMs by using DevTest Labs.

- Contoso already has the [Azure infrastructure](#) in place, including the development virtual network.
- With everything prepared, Contoso will provision and configure DevTest Labs.
- Contoso will configure the development virtual network, assign a resource group, and set policies.
- Contoso will create Windows Virtual Desktop instances for developers to use at remote locations.
- Contoso will create VMs within DevTest Labs for development and migrate databases.

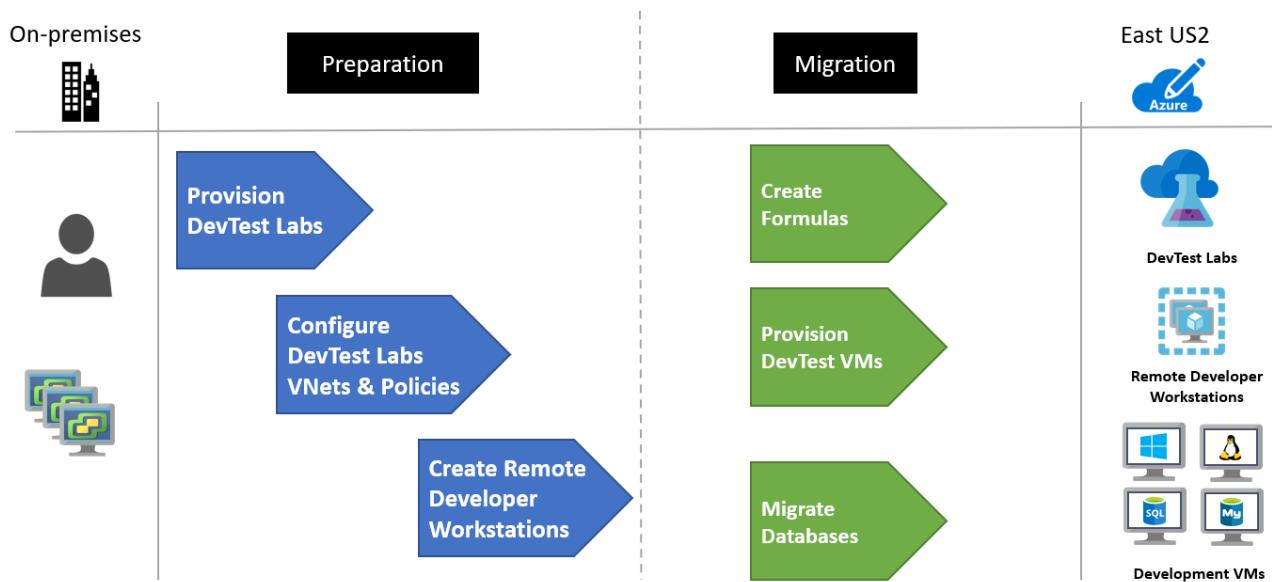


Figure 2: The migration process.

## Prerequisites

Here's what Contoso needs to run this scenario.

REQUIREMENTS	DETAILS
--------------	---------

Requirements	Details
Azure Dev/Test subscription	<p>Contoso creates an <a href="#">Azure Dev/Test subscription</a> to reduce costs up to 80 percent.</p> <p>If you don't have an Azure subscription, create a <a href="#">free account</a>.</p> <p>If you create a free account, you're the admin of your subscription and can perform all actions.</p> <p>If you use an existing subscription and you're not the admin, work with the admin to assign you Owner or Contributor permissions.</p> <p>If you need more granular permissions, review <a href="#">Manage Site Recovery access with Azure role-based access control</a>.</p>
Azure infrastructure	Learn how Contoso <a href="#">set up an Azure infrastructure</a> .

## Scenario steps

Here's how Contoso admins will run the migration:

- Step 1: Provision a new Azure Dev/Test subscription and create a DevTest Labs instance.
- Step 2: Configure the development virtual network, assign a resource group, and set policies.
- Step 3: Create Windows 10 Enterprise multi-session virtual desktops for developers to use from remote locations.
- Step 4: Create formulas and VMs within DevTest Labs for development and migrate databases.

## Step 1: Provision a new Azure Dev/Test subscription and create a DevTest Labs instance

Contoso admins first need to provision a new subscription by using the Azure Dev/Test offer, and then create a DevTest Labs instance.

They set these up as follows:

The admins follow the link to the [Azure Dev/Test subscription offer](#) and provision a new subscription, which saves them up to 80 percent on their systems. This offer allows them to run Windows 10 images on Azure for dev/test. They will gain access to [Windows Virtual Desktop](#) to simplify the management experience of the remote developers.



Figure 3: An Azure Dev/Test subscription offer.

With their new subscription provisioned, Contoso admins use the Azure portal to create a new DevTest Labs instance. The new lab is created in the `ContosoDevRG` resource group.

## DevTest Labs

Microsoft

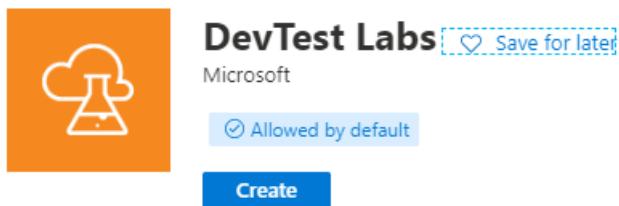


Figure 4: Creating a new DevTest Labs instance.

## Step 2: Configure the development virtual network, assign a resource group, and set policies

With the DevTest Labs instance created, Contoso performs the following configurations:

1. Configure the virtual network:

- a. In the portal, Contoso opens the DevTest Labs instance and selects **Configuration and policies**.

The screenshot shows the 'My Lab' interface for the 'ContosoDevTestLabs' DevTest Lab. The left sidebar includes links for Overview, Getting started, Internal support, My virtual machines, Claimable virtual machines, All virtual machines, Security alerts, My data disks, Formulas (reusable bases), My secrets, and Personal data. The 'Settings' section contains a link to 'Configuration and policies', which is highlighted with a red rectangular box.

Figure 5: DevTest Labs instance: configuration and policies.

- b. Contoso selects **Virtual Networks > + Add**, chooses `vnet-dev-eus2`, and then selects **Save**. This allows the development virtual network to be used for VM deployments. A virtual network was also created during the deployment of the DevTest Labs instance.

Name	Resource group	Status
vnet-dev-eus2	contosonetworking	Ready
dtlcontosodevtestlabs	contosodevrg	Ready

Figure 6: Virtual networks.

## 2. Assign a resource group:

- To ensure that resources are deployed to the `ContosoDevRG` resource group, Contoso configures this in the lab settings. It also assigns its developers the **Contributor** role.

Figure 7: Assigning a resource group.

### NOTE

The Contributor role is an administrator-level role with all rights except the ability to provide access to other users. Read more about [Azure role-based access control](#).

## 3. Set lab policies:

- Contoso needs to ensure that its developers are using DevTest Labs within team policies. Contoso configures DevTest Labs with these policies.
- Contoso enables auto-shutdown with a local time of 7:00:00 PM and the correct time zone.

Enabled

Scheduled shutdown

7:00:00 PM

Time zone

(UTC-05:00) Eastern Time (US & Canada)

Send notification before auto-shutdown?

Figure 8: Auto-shutdown.

- c. Contoso enables auto-start to have the VMs running when the developers come online to work. They're configured to the local time zone and for the days of the week when the developers work.

Scheduled start

7:00:00 AM

Time zone

(UTC-05:00) Eastern Time (US & Canada)

<input type="checkbox"/> Day of week	Time
<input checked="" type="checkbox"/> Monday	07:00:00
<input checked="" type="checkbox"/> Tuesday	07:00:00
<input checked="" type="checkbox"/> Wednesday	07:00:00
<input checked="" type="checkbox"/> Thursday	07:00:00
<input checked="" type="checkbox"/> Friday	07:00:00
<input type="checkbox"/> Saturday	07:00:00
<input type="checkbox"/> Sunday	07:00:00

Figure 9: Auto-start.

- d. Contoso configures the allowed VM sizes, ensuring that large and expensive VMs can't be started.



Enabled

On     Off

- Name
- Standard\_B1ls
- Standard\_B1ms
- Standard\_B1s
- Standard\_B2ms
- Standard\_B2s
- Standard\_B4ms
- Standard\_B8ms
- Standard\_B12ms
- Standard\_B16ms
- Standard\_B20ms
- Standard\_D1\_v2
- Standard\_D2\_v2
- Standard\_D3\_v2

Figure 10: Allowed VM sizes.

- e. Contoso configures the support message.

The screenshot shows the 'Configuration and policies | Internal support' page for a 'DevTest Lab'. The left sidebar has a 'Settings' section with options like 'Internal support', 'Allowed virtual machine sizes', 'Virtual machines per user', 'Virtual machines per lab', 'Lab settings', 'Lab announcement', 'Identity (Preview)', and 'Schedules'. Under 'Internal support', there is a search bar, 'Save' and 'Feedback' buttons, and a note: 'Enter text here to have it displayed in the Internal Support link'. Below this is a note: 'The support message supports markdown. Click for more information.' A 'Enabled' switch is set to 'Yes'. The 'Support message' field contains the text: 'Welcome to the Contoso DevTest Labs instance in Azure! If you have issues please use the ContosoDevTestLabs support Channel in Teams.'

Figure 11: A support message.

## Step 3: Create Windows 10 Enterprise multi-session virtual desktops for developers to use from remote locations

Contoso needs to create a Windows Virtual Desktop base for remote developers.

1. Contoso selects All virtual machines > + Add and chooses a Windows 10 Enterprise multi-session base for a VM.

## Choose a base

-  Windows 10 Enterprise multi-session, Version 1903 + Office 365 ProPlus
-  Windows 10 Enterprise multi-session, Version 1909 + Office 365 ProPlus
-  Windows 10 Enterprise multi-session, Version 2004 + Office 365 ProPlus
-  Windows 10 Enterprise multi-session, Version 1809 + Office 365 ProPlus

Figure 12: A Windows 10 Enterprise multi-session base.

2. Contoso configures the size of the VM along with the artifacts to be installed. In this case, the developers have access to common development tools such as Visual Studio Code, Git, and Chocolatey.

## Selected artifacts

Name	
 Visual Studio Code	...
 git	...
 7-Zip	...
 Install Chocolatey Packages	...
 PuTTY	...

Figure 13: Artifacts.

3. Contoso reviews the VM configuration for accuracy.

## Create virtual machine from formula

Virtual machine

Basic Settings      Advanced Settings

User Settings

Virtual machine name: RemoteDevs

Description:

User name \*: remotedevs

Use a saved secret:

Password \*: ..... ✓

Save as default password:

Base Image Information

Image Base Selection

**Base**  
Windows 10 Enterprise multi-session, Version 2004 + Office 365 ProPlus  
[Choose a base](#)

Disk and Size

Virtual machine size \*:  Standard\_DS2\_v2 [Change Size](#)

OS disk type: Premium SSD

Artifacts

Artifacts Selection

**Artifact**  
6 artifact(s) selected  
[Add or Remove Artifacts](#)

Figure 14: Create a virtual machine from a base.

- After the VM is created, Contoso's remote developers can connect to and use this development workstation for their work. The selected artifacts are installed, saving developers time in configuring their workstation.

RemoteDevs | Overview

virtual machine

Search (Ctrl+ /) Connect Start Restart Stop Artifacts Claim machine Unclaim Delete

General

Running

Resource group : contosodevrg  
Virtual network/subnet :  
IP address or FQDN : contosodevtestlabs.eastus2.cloudapp.azure.com  
NAT protocol / Port to co... : RDP / 59468

Operations

Create custom image

Figure 15: A remote developer VM.

## Step 4: Create formulas and VMs within DevTest Labs for development and migrate databases

With DevTest Labs configured and the remote developers' workstation up and running, Contoso focuses on building its VMs for development. To get started, Contoso completes the following steps:

1. Contoso creates formulas (reusable bases) for application and database VMs, and it provisions application and database VMs by using the formulas.

Contoso selects **Formulas** > **+ Add**, and then a **Windows Server 2012 R2 Datacenter** base.

[Home](#) > [DevTest Labs](#) > [ContosoDevTestLabs | Formulas \(reusable bases\)](#) >

## Choose a base

 SUSE	SUSE Linux Enterprise Server (SLES) for SAP Applications 15 SP1 with 24x7 Integrated Support
 GEN2:	SUSE Enterprise Linux for SAP 12 SP4 - BYOS
 GEN2:	SUSE Enterprise Linux for SAP 15 - BYOS
 GEN2:	SUSE Enterprise Linux for SAP 15 +24x7 Support
 [smalldisk]	Windows Server 2008 R2 SP1
 [smalldisk]	Windows Server 2012 Datacenter
 [smalldisk]	Windows Server 2012 R2 Datacenter

*Figure 16: A Windows 2012 R2 base.*

2. Contoso configures the size of the VM along with the artifacts to be installed. In this case, the developers have access to common development tools such as Visual Studio Code, Git, and Chocolatey.

## Create formula (reusable base)

Create a formula to capture the settings used to create this virtual machine.

Basic Settings    Advanced Settings

User Settings

Formula name  ✓

Description  ✓

User name  ✓

Use a saved secret

Secret  ✓

Disk and Size

Virtual machine size (i)

Size  Change Size

OS disk type (i)  ✓

Artifacts

Artifacts Selection

Artifact  Add or Remove Artifacts

Figure 17: A Windows 2012 R2 base configuration.

3. To create the database VM formula, Contoso follows the same basic steps. This time, it selects a SQL Server 2012 image for the base.

[Home](#) > [DevTest Labs](#) > [ContosoDevTestLabs | Formulas \(reusable bases\)](#) >

## Choose a base

- {BYOL} SQL Server 2012 SP4 Standard on Windows Server 2012 R2
- {BYOL} SQL Server 2016 SP1 Enterprise on Windows Server 2016
- {BYOL} SQL Server 2016 SP1 Standard on Windows Server 2016
- {BYOL} SQL Server 2016 SP2 Enterprise on Windows Server 2016
- {BYOL} SQL Server 2016 SP2 Standard on Windows Server 2016
- {BYOL} SQL Server 2017 Enterprise Windows Server 2016
- {BYOL} SQL Server 2017 Standard on Windows Server 2016

Figure 18: A SQL Server 2012 image.

4. Contoso configures the formula with the size and artifacts. The artifacts include SQL Server Management Studio, which is required for this database development VM formula.

## Create formula (reusable base)

Create a formula to capture the settings used to create this virtual machine.

[Basic Settings](#)   [Advanced Settings](#)

User Settings

Formula name

SQLDbDevVmBase



Description

This base should be used for SQL Server 2012 R2 database development



User name

RemoteDev



Use a saved secret



Secret

VmPassword



Disk and Size

Virtual machine size (i)

**Size**

Standard\_B2ms

[Change Size](#)

OS disk type (i)

Standard SSD



Artifacts

Artifacts Selection

**Artifact**

1 artifact(s) selected

[Add or Remove Artifacts](#)

Figure 19: An SQL 2020 R2 base configuration.

Learn more about [using formulas with Azure DevTest Labs](#).

- Contoso has now created the Windows base formulas for its developers to use for applications and databases.

**ContosoDevTestLabs | Formulas (reusable bases)**

DevTest Lab

+ Add

Overview
Getting started
Internal support

My Lab

Name	Status	Description
Win2012AppDevVmBase	Ready	This base should be used for Windows 2012 R2 based application development
SQLDbDevVmBase	Ready	This base should be used for SQL Server 2012 R2 database development

Figure 20: Windows base formulas.

The next steps provision application and database VMs through the formulas:

- With the formulas created, Contoso next selects **All virtual machines** and then the **Windows2012AppDevVmBase** formula to match the configuration of its current application development VMs.

## Choose a base

-  Web App with SQL Database
-  Win2012AppDevVmBase
-  Ubuntu Server 19.10
-  Ubuntu Server 20.04 LTS

Figure 21: An application development VM.

- Contoso configures the VM with the size and artifacts that are required for this application VM.

## Create virtual machine from formula

Virtual machine

Basic Settings    Advanced Settings

User Settings

Virtual machine name  

Description: This base should be used for Windows 2012 R2 based application development

User name \*

Use a saved secret

Secret \*

Base Image Information

Image Base Selection

Base  
[smalldisk] Windows Server 2012 R2 Datacenter  
[Choose a base](#)

Disk and Size

Virtual machine size \* 

Size  
Standard\_B2ms  
[Change Size](#)

OS disk type 



Artifacts

Artifacts Selection

Artifact  
3 artifact(s) selected  
[Add or Remove Artifacts](#)

Figure 22: Size and artifact configurations for a VM.

- Contoso provisions the database VM by using the **SQLDbDevVmBase** formula to match the configuration of its current database development VMs.

## Choose a base



Figure 23: A database VM.

4. Contoso configures the VM with the size and artifacts that are required.

## Create virtual machine from formula

Virtual machine

The screenshot displays the configuration interface for creating a new virtual machine. It includes fields for basic settings like user name and password, and advanced settings for base image, disk size, and artifacts.

**User Settings:**  
Virtual machine name: SQLDbDevVm1  
User name \*: RemoteDev  
Use a saved secret:   
Secret \*: VmPassword

**Base Image Information:**  
Image Base Selection:  
Base: {BYOL} SQL Server 2012 SP4 Standard on Windows Server 2012 R2  
Choose a base

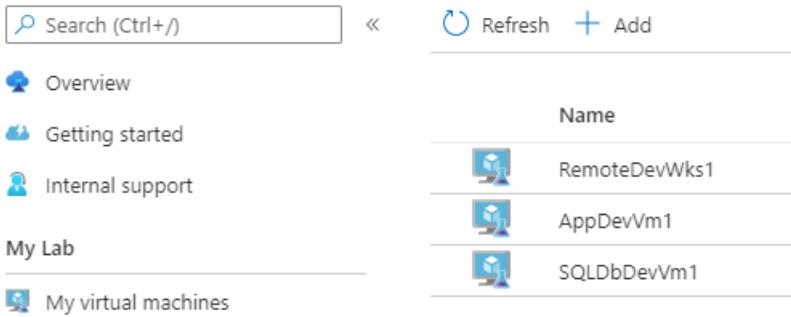
**Disk and Size:**  
Virtual machine size \*:  (Standard\_B2ms)  
OS disk type: Standard SSD

**Artifacts:**  
Artifacts Selection:  
Artifact: 1 artifact(s) selected  
Add or Remove Artifacts

Figure 24: Database configurations for a VM.

5. With the first VMs created along with the remote developers' workstation, Contoso's developers are ready to start writing code in Azure.

## ContosoDevTestLabs | All virtual machines DevTest Lab



Name
RemoteDevWks1
AppDevVm1
SQLDbDevVm1

Figure 25: Contoso VMs.

6. Contoso can now restore its development databases either from backups or by using some type of code generation process to build the schema on the VMs. With SQL Server Management Studio already installed through the artifacts, these are simple tasks that don't require installing any tools.

## Clean up after migration

Contoso will continue using these steps to migrate its VMs to Azure by using DevTest Labs. With each migration complete, all development VMs are now running in DevTest Labs.

Now, Contoso needs to complete these cleanup steps:

- Remove the VMs from the vCenter inventory.
- Remove all the VMs from local backup jobs.
- Update internal documentation to show the new location and IP addresses for the VMs.
- Review any resources that interact with the VMs, and update any relevant settings or documentation to reflect the new configuration.

### Security

The Contoso security team reviews the Azure VMs to determine any security issues. To control access, the team reviews the network security groups (NSGs) for the VMs. NSGs are used to ensure that only traffic allowed to the application can reach it. The team also considers securing the data on the disk by using Azure Disk Encryption and Azure Key Vault. For more information, see [Security best practices for IaaS workloads in Azure](#).

### Licensing and cost optimization

- Contoso will ensure that all development Azure resources are created through this dev/test subscription to take advantage of the 80 percent savings.
- Budgets will be reviewed for all DevTest Labs instances and policies for the VMs to ensure that costs are contained and overprovisioning doesn't happen mistakenly.
- Contoso will enable [Azure Cost Management + Billing](#) to help monitor and manage the Azure resources.

## Conclusion

In this article, Contoso moved its development environments to DevTest Labs. It also implemented Windows Virtual Desktop as a platform for remote and contract developers.

### Need more help?

[Create a DevTest Labs instance](#) in your subscription now, and learn how to use DevTest Labs for developers.

# Migrate an application to Azure App Service and SQL Database

11/9/2020 • 15 minutes to read • [Edit Online](#)

This article demonstrates how the fictional company Contoso refactors a two-tier Windows .NET application that's running on VMware VMs as part of a migration to Azure. The Contoso team migrates the application front-end virtual machine (VM) to an Azure App Service web app and the application database to Azure SQL Database.

The SmartHotel360 application that we use in this example is provided as open source. If you want to use it for your own testing purposes, you can download it from [GitHub](#).

## Business drivers

The Contoso IT leadership team has worked closely with business partners to understand what they want to achieve with this migration:

- **Address business growth.** Contoso is growing, and there is pressure on their on-premises systems and infrastructure.
- **Increase efficiency.** Contoso needs to remove unnecessary procedures and streamline processes for developers and users. The business needs IT to be fast and not waste time or money, thus delivering faster on customer requirements.
- **Increase agility.** To enable their success in a global economy, Contoso IT needs to be more responsive to the needs of the business. It must be able to react more quickly to changes in the marketplace. IT must not get in the way or become a business blocker.
- **Scale.** As the business grows successfully, Contoso IT must provide systems that are able to grow at the same pace.
- **Reduce costs.** Contoso wants to minimize licensing costs.

## Migration goals

To help determine the best migration method, the Contoso cloud team pinned down the following goals:

REQUIREMENTS	DETAILS

Requirements	Details
<b>Application</b>	<p>The application in Azure will remain as critical as it is today on-premises.</p> <p>It should have the same performance capabilities as it currently does in VMware.</p> <p>The team doesn't want to invest in the application. For now, admins will simply move the application safely to the cloud.</p> <p>The team wants to stop supporting Windows Server 2008 R2, which the application currently runs on.</p> <p>The team also wants to move away from SQL Server 2008 R2 to a modern platform as a service (PaaS) database, which will minimize the need for management.</p> <p>Contoso wants to take advantage of its investment in SQL Server licensing and Software Assurance where possible.</p> <p>In addition, Contoso wants to mitigate the single point of failure on the web tier.</p>
<b>Limitations</b>	<p>The application consists of an ASP.NET application and a Windows Communication Foundation (WCF) service running on the same VM. They want to spread these components across two web apps using the Azure App Service.</p>
<b>Azure</b>	<p>Contoso wants to move the application to Azure, but they don't want to run it on VMs. Contoso wants to use Azure PaaS services for both the web and data tiers.</p>
<b>DevOps</b>	<p>Contoso wants to move to a DevOps model that uses Azure DevOps for their builds and release pipelines.</p>

## Solution design

After pinning down their goals and requirements, Contoso designs and reviews a deployment solution. They also identify the migration process, including the Azure services that they'll use for the migration.

### Current application

- The SmartHotel360 on-premises application is tiered across two VMs, `WEBVM` and `SQLVM`.
- The VMs are located on VMware ESXi host `contosohost1.contoso.com` version 6.5.
- The VMware environment is managed by vCenter Server 6.5 (`vcenter.contoso.com`), which runs on a VM.
- Contoso has an on-premises datacenter (`contoso-datacenter`), with an on-premises domain controller (`contosodc1`).
- The on-premises VMs in the Contoso datacenter will be decommissioned after the migration is done.

### Proposed solution

- For the database tier of the application, Contoso compared Azure SQL Database to SQL Server by referring to [Features comparison: Azure SQL Database and Azure SQL Managed Instance](#). Contoso decided to use Azure SQL Database for a few reasons:
  - Azure SQL Database is a managed relational database service. It delivers predictable performance at multiple service levels, with near-zero administration. Advantages include dynamic scalability with no downtime, built-in intelligent optimization, and global scalability and availability.

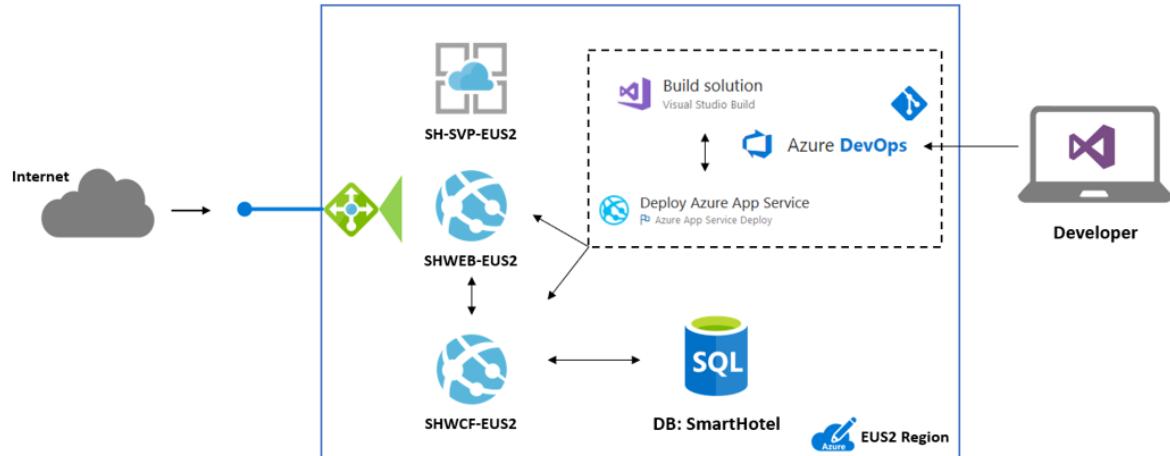
- Contoso can use the lightweight Data Migration Assistant to assess the on-premises database migration to Azure SQL.
  - Contoso can use Azure Database Migration Service to migrate the on-premises database to Azure SQL.
  - With Software Assurance, Contoso can exchange existing licenses for discounted rates on a database in SQL Database by using the Azure Hybrid Benefit for SQL Server. This approach could provide a cost saving of up to 30 percent.
  - SQL Database provides security features such as Always Encrypted, dynamic data masking, row-level security, and SQL threat detection.
- For the application web tier, Contoso has decided to use Azure App Service. This PaaS service enables them to deploy the application with just a few configuration changes. Contoso will use Visual Studio to make the change, and they'll deploy two web apps, one for the website and one for the WCF service.
  - To meet requirements for a DevOps pipeline, Contoso will use Azure DevOps for source code management with Git repos. They'll use automated builds and release to build the code and deploy it to the Azure App Service.

## Solution review

Contoso evaluates their proposed design by putting together a pros and cons list, as shown in the following table:

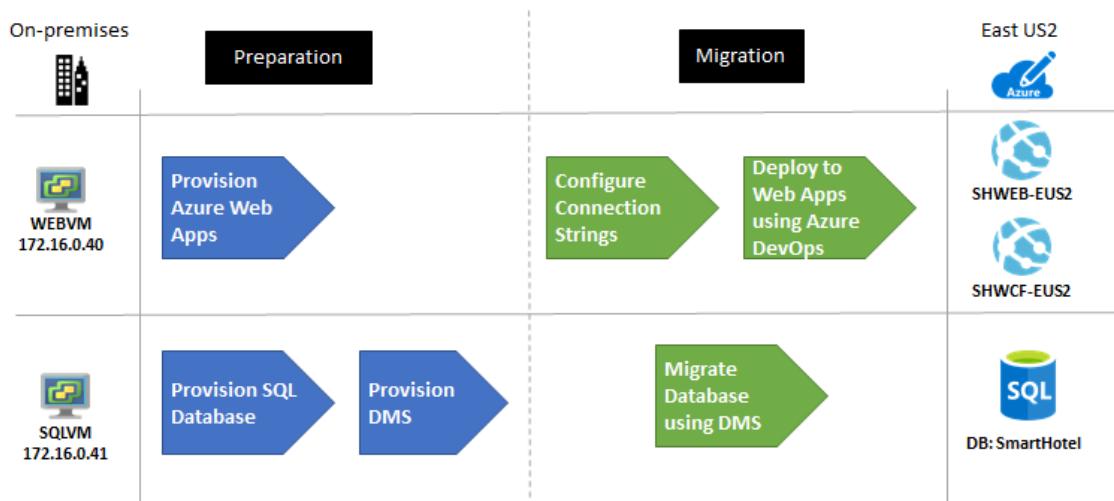
CONSIDERATION	DETAILS
Pros	<p>The SmartHotel360 application code doesn't require changes for migration to Azure.</p> <p>Contoso can take advantage of their investment in Software Assurance by using the Azure Hybrid Benefit for both SQL Server and Windows Server.</p> <p>After the migration, Windows Server 2008 R2 won't need to be supported. For more information, see the <a href="#">Microsoft Lifecycle Policy</a>.</p> <p>Contoso can configure the web tier of the application with multiple instances, so that the web tier is no longer a single point of failure.</p> <p>The database will no longer depend on the aging SQL Server 2008 R2.</p> <p>SQL Database supports the technical requirements. Contoso assessed the on-premises database by using Data Migration Assistant and found that it's compatible.</p> <p>Azure SQL Database has built-in fault tolerance that Contoso doesn't have to set up. This ensures that the data tier is no longer a single point of failover.</p> <p>If Contoso uses Azure Database Migration Service to migrate their database, it will have the infrastructure ready for migrating databases at scale.</p>
Cons	<p>Azure App Service supports only one application deployment for each web app. This means that two web apps must be provisioned, one for the website and one for the WCF service.</p>

## Proposed architecture



## Migration process

1. Contoso provisions an Azure SQL managed instance and then migrates the SmartHotel360 database to it by using Azure Database Migration Service.
2. Contoso provisions and configures web apps, and deploys the SmartHotel360 application to them.



## Azure services

SERVICE	DESCRIPTION	COST
Azure App Service Migration Assistant	A free and simple path to seamlessly migrate .NET web applications from on-premises to the cloud with minimal to no code changes.	It's a downloadable tool, free of charge.
Data Migration Assistant	Contoso will use Data Migration Assistant to assess and detect compatibility issues that might affect database functionality in Azure. Data Migration Assistant assesses feature parity between SQL sources and targets, and it recommends performance and reliability improvements.	It's a downloadable tool, free of charge.

Service	Description	Cost
Azure Database Migration Service	Azure Database Migration Service enables seamless migration from multiple database sources to Azure data platforms with minimal downtime.	Learn about <a href="#">supported regions</a> and <a href="#">Database Migration Service pricing</a> .
Azure SQL Database	An intelligent, fully managed relational cloud database service.	Cost is based on features, throughput, and size. <a href="#">Learn more</a> .
Azure App Service	Helps create powerful cloud applications that use a fully managed platform.	Pricing is based on size, location, and usage duration. <a href="#">Learn more</a> .
Azure DevOps	Provides a continuous integration and continuous deployment (CI/CD) pipeline for application development. The pipeline starts with a Git repository for managing application code, a build system for producing packages and other build artifacts, and a release management system to deploy changes in dev, test, and production environments.	

## Prerequisites

To run this scenario, Contoso must meet the following prerequisites:

Requirements	Details
Azure subscription	Contoso created subscriptions earlier in this article series. If you don't have an Azure subscription, create a <a href="#">free account</a> .  If you create a free account, you're the administrator of your subscription and can perform all actions.  If you use an existing subscription and you're not the administrator, you need to work with the admin to assign you Owner or Contributor permissions.
Azure infrastructure	Contoso set up their Azure infrastructure as described in <a href="#">Azure infrastructure for migration</a> .

## Scenario steps

Here's how Contoso will run the migration:

- **Step 1: Assess and migrate the web apps..** Contoso uses the [Azure App Service Migration Assistant](#) tool to

run pre-migration compatibility checks and migrate their web apps to Azure App Service.

- **Step 2: Provision a database in Azure SQL Database.** Contoso provisions an Azure SQL Database instance. After the application website is migrated to Azure, the WCF service web app will point to this instance.
- **Step 3: Assess the database.** Contoso assesses the database for migration by using Data Migration Assistant and then migrates it via Azure Database Migration Service.
- **Step 4: Set up Azure DevOps.** Contoso creates a new Azure DevOps project, and imports the Git repo.
- **Step 5: Configure connection strings.** Contoso configures connection strings so that the web tier web app, the WCF service web app, and the SQL instance can communicate.
- **Step 6: Set up build and release pipelines in Azure DevOps.** As a final step, Contoso sets up build and release pipelines in Azure DevOps to create the application, and then deploys them to two separate web apps.

## Step 1: Assess and migrate the web apps

Contoso admins assess and migrate their web app using the [Azure App Service Migration Assistant](#) tool. They use the [Migrate ASP.NET Apps to Azure learning path](#) as a guide during the process. The admins perform these actions:

- They use the Azure [App Service Migration Assessment](#) tool to evaluate any dependencies between their web apps and to determine if there are any incompatibilities between their on-premises web apps and what's supported on Azure App Service.
- They download the Azure App Service Migration Assistant and sign in to their Azure account.
- They choose a subscription, a resource group, and the website's domain name.

## Step 2: Provision a database in Azure SQL Database

1. Contoso admins decide to create an Azure SQL Database instance.

The screenshot shows the Azure Marketplace search results for 'Databases'. A red box highlights the 'SQL Database' option, which includes a 'Quickstart tutorial'. Other options listed include 'SQL Data Warehouse', 'SQL Elastic database pool', 'Azure Database for MySQL', and 'Azure Database for PostgreSQL'. The 'Databases' category is also highlighted with a blue box.

2. They specify a database name to match the database, `SmartHotel.Registration`, that's running on the on-premises VM. They place the database in the ContosoRG resource group. This is the resource group they use for production resources in Azure.

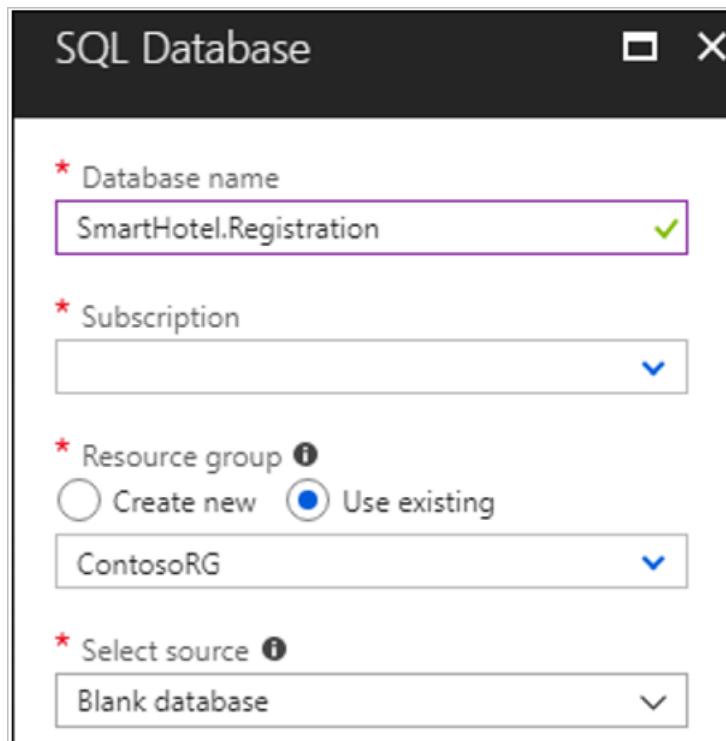
SQL Database

\* Database name  
SmartHotel.Registration ✓

\* Subscription  
▼

\* Resource group ⓘ  
 Create new  Use existing  
ContosoRG ▼

\* Select source ⓘ  
Blank database ▼



3. They set up a new SQL Server instance, sql-smarthotel-eus2, in the primary region.

New server

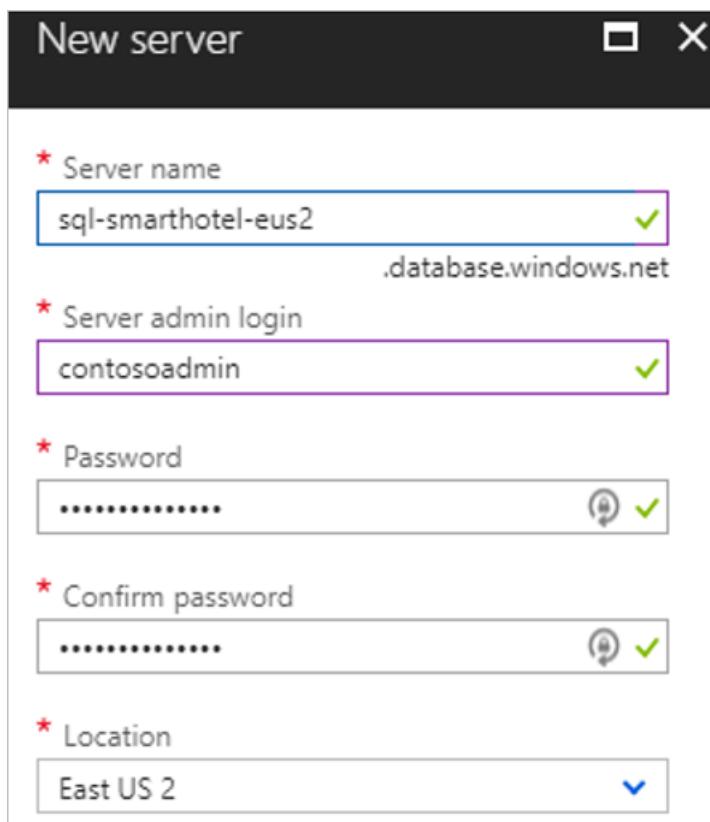
\* Server name  
sql-smarthotel-eus2 .database.windows.net ✓

\* Server admin login  
contosoadmin ✓

\* Password  
\*\*\*\*\* 🔒 ✓

\* Confirm password  
\*\*\*\*\* 🔒 ✓

\* Location  
East US 2 ▼



4. They set the pricing tier to match their server and database needs. And they select to save money with Azure Hybrid Benefit because they already have a SQL Server license.
5. For sizing, they use vCore-based purchasing and set the limits for their expected requirements.

## Compute Generation i

**Gen4**



up to 24 vCores

up to 168 GB memory

## Save money

Save up to 30% with a license you already own. Already have a SQL Server license? i

Yes  No

### LICENSE TYPE

SQL server

I confirm that I have a SQL server license with Software Assurance to apply this Azure Hybrid Benefit for SQL Server

vCores [How do vCores compare with DTUs?](#) i



Max data size i



6. They create the database instance.

**SQL Database**

\* Database name  
SmartHotel.Registration ✓

\* Subscription  
▼

\* Resource group ⓘ  
 Create new  Use existing  
ContosoRG ▼

\* Select source ⓘ  
Blank database ▼

---

\* Server  
sql-smarthotel-eus2 (East US 2) >

---

Want to use SQL elastic pool? ⓘ  
 Yes  Not now

---

\* Pricing tier ⓘ  
General Purpose: Gen4, 4 vCores,... >

---

\* Collation ⓘ  
SQL\_Latin1\_General\_CI\_AS

- They open the database and note the details they'll need when they use Data Migration Assistant for migration.

```
smarthotelsqldb.txt - Notepad
File Edit Format View Help
Server: sql-smarthotel-eus2.database.windows.net
User: contosoadmin
Password: XXXXXXXX
Database: SmartHotel.Registration|
```

Need more help?

- [Get help provisioning a SQL Database.](#)
- Learn about [vCore resource limits](#).

## Step 3: Assess the database

Contoso admins assess the database by using Data Migration Assistant and then migrate it by using Azure

Database Migration Service by referring to the [step-by-step migration tutorial](#). They can perform online, offline, and hybrid (preview) migrations.

In brief, the admins do the following:

- They use Data Migration Assistant to discover and resolve any database migration issues.
- They create an Azure Database Migration Service instance with a Premium SKU that's connected to the virtual network.
- They ensure that the instance can access the remote SQL Server via the virtual network. This entails ensuring that all incoming ports are allowed from Azure to SQL Server at the virtual network level, the network VPN, and the machine that hosts SQL Server.
- They configure the instance:
  - Create a migration project.
  - Add a source (on-premises database).
  - Select a target.
  - Select the databases to migrate.
  - Configure advanced settings.
  - Start the replication.
  - Resolve any errors.
  - Perform the final cutover.

## Step 4: Set up Azure DevOps

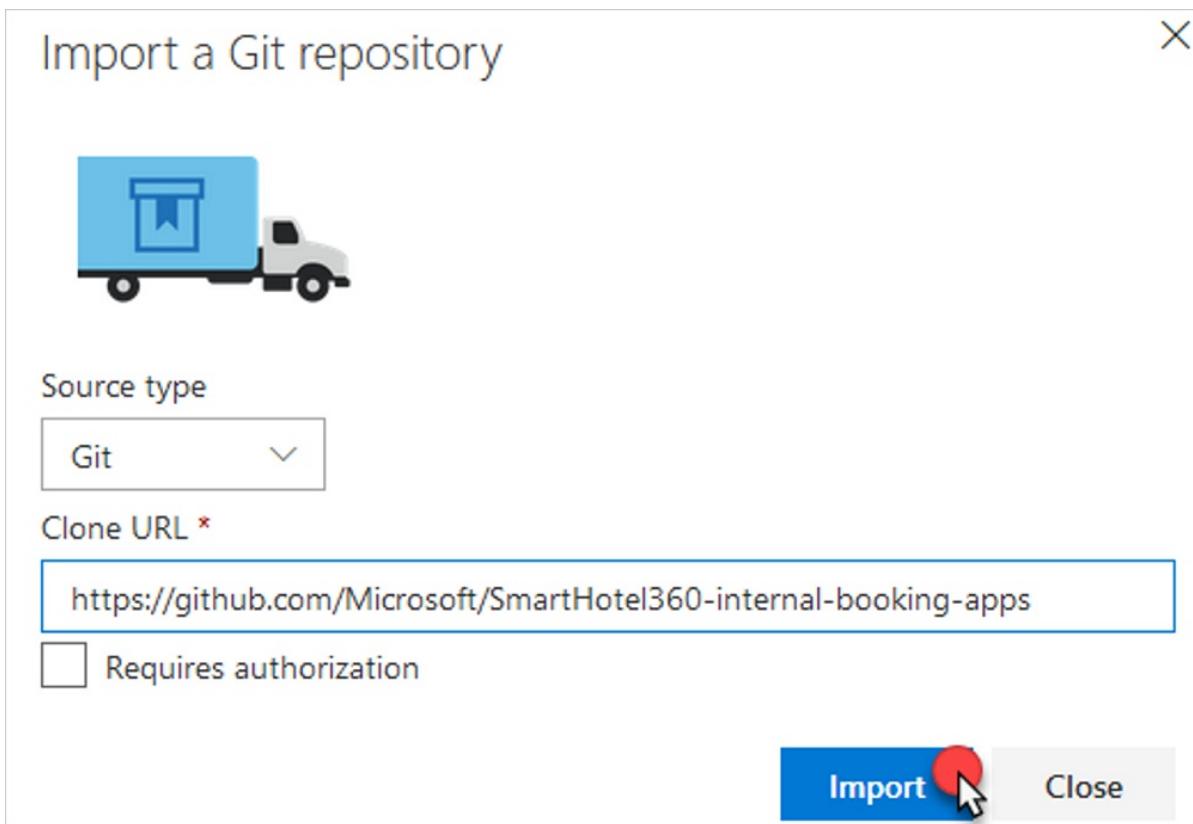
Contoso needs to build the DevOps infrastructure and pipelines for the application. To do this, Contoso admins create a new DevOps project, import the code, and then set up build and release pipelines.

1. In the Contoso Azure DevOps account, they create a new project, **ContosoSmartHotelRefactor**, and then select **Git** for version control.

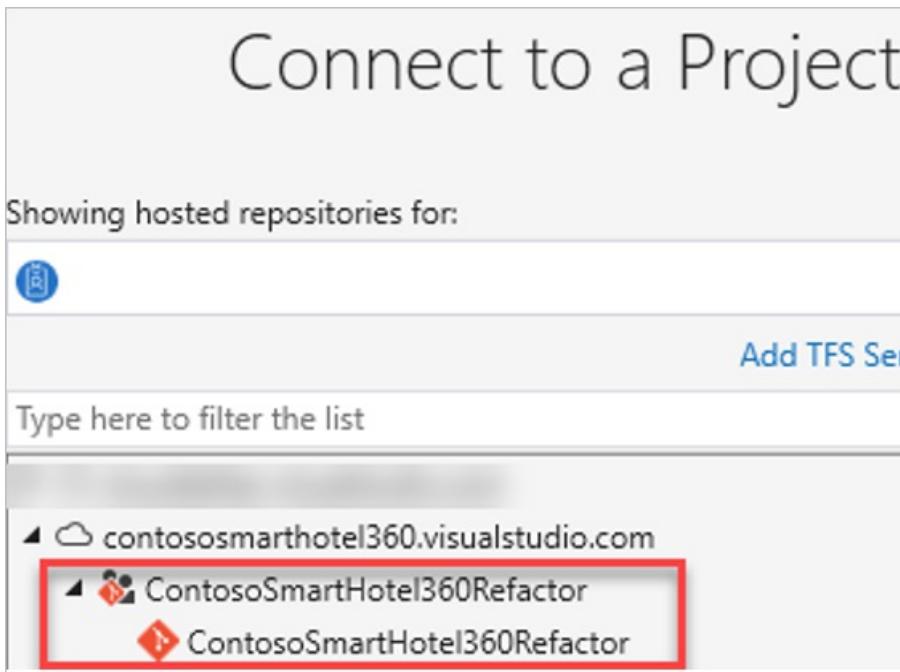
The screenshot shows the 'Create a new project' wizard in the Azure DevOps interface. The 'Project name' field is filled with 'SmartHotel360Rearchitect'. The 'Description' field is empty. In the 'Visibility' section, the 'Public' option is shown with a description: 'Anyone on the internet can view the project. Certain features like TFVC are not supported.' The 'Private' option is selected, indicated by a blue border around its button and a checked radio button. Its description states: 'Only people you give access to will be able to view this project.'

<b>Project name *</b>
SmartHotel360Rearchitect
<b>Description</b>
(empty text area)
<b>Visibility</b>
<input type="radio"/> <b>Public</b> ⓘ
Anyone on the internet can view the project. Certain features like TFVC are not supported.
<input checked="" type="radio"/> <b>Private</b>
Only people you give access to will be able to view this project.

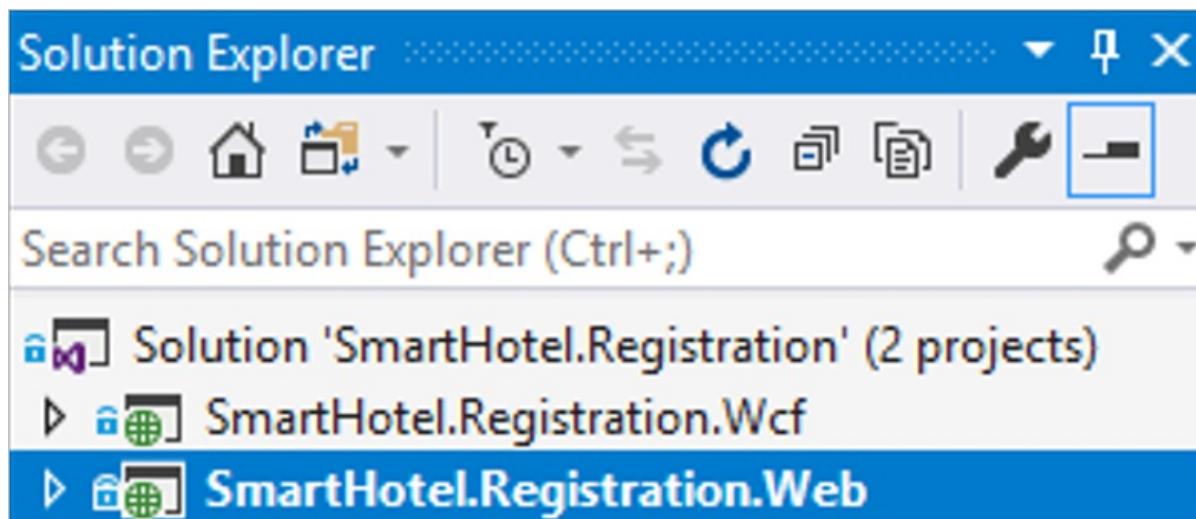
2. They import the Git repo that currently holds their application code. They download it from the [public GitHub repository](#).



3. They connect Visual Studio to the repo and then clone the code to the developer machine by using Team Explorer.



4. They open the solution file for the application. The web app and the WCF service have separate projects within the file.



## Step 5: Configure connection strings

The Contoso admins make sure that the web apps and database can communicate with each other. To do this, they configure connection strings in the code and in the web apps.

1. In the web app for the WCF service, `SHWCF-EUS2`, under **Settings > Application settings**, they add a new connection string named **DefaultConnection**.
2. They pull the connection string from the SmartHotel-Registration database and then update it with the correct credentials.

The screenshot shows the 'SmartHotel-Registration - Connection strings' page in the Azure portal. On the left, there's a sidebar with links like Overview, Activity log, Tags, Diagnose and solve problems, Quick start, and Query editor (preview). Below that is a 'SETTINGS' section with Configure, Geo-Replication, and Connection strings. The 'Connection strings' link is highlighted with a red box. The main area shows an ADO.NET tab with a connection string configuration. The connection string details are:  
ADO.NET (SQL authentication)  
Server=tcp:sql-smarthotel-eus2.database.windows.net,1433;Initial Catalog=SmartHotel\_Web;User ID=sa;Password={your\_password};MultipleActiveResultSets=False;Encrypt=True;TrustServerCertificate=False;Connection Timeout=30;  
[Download ADO.NET driver for SQL server](#)

3. In Visual Studio, the admins open the `SmartHotel.Registration.wcf` project from the solution file. In the

project, they update the `connectionStrings` section of the `web.config` file with the connection string.

```
<connectionStrings>
  <add name="DefaultConnection" connectionString="Server=tcp:sql-smarthotel-eus2.</connectionStrings>
```

4. They change the `client` section of the `web.config` file for `SmartHotel.Registration.Web` to point to the new location of the WCF service. This is the URL of the WCF web app that hosts the service endpoint.

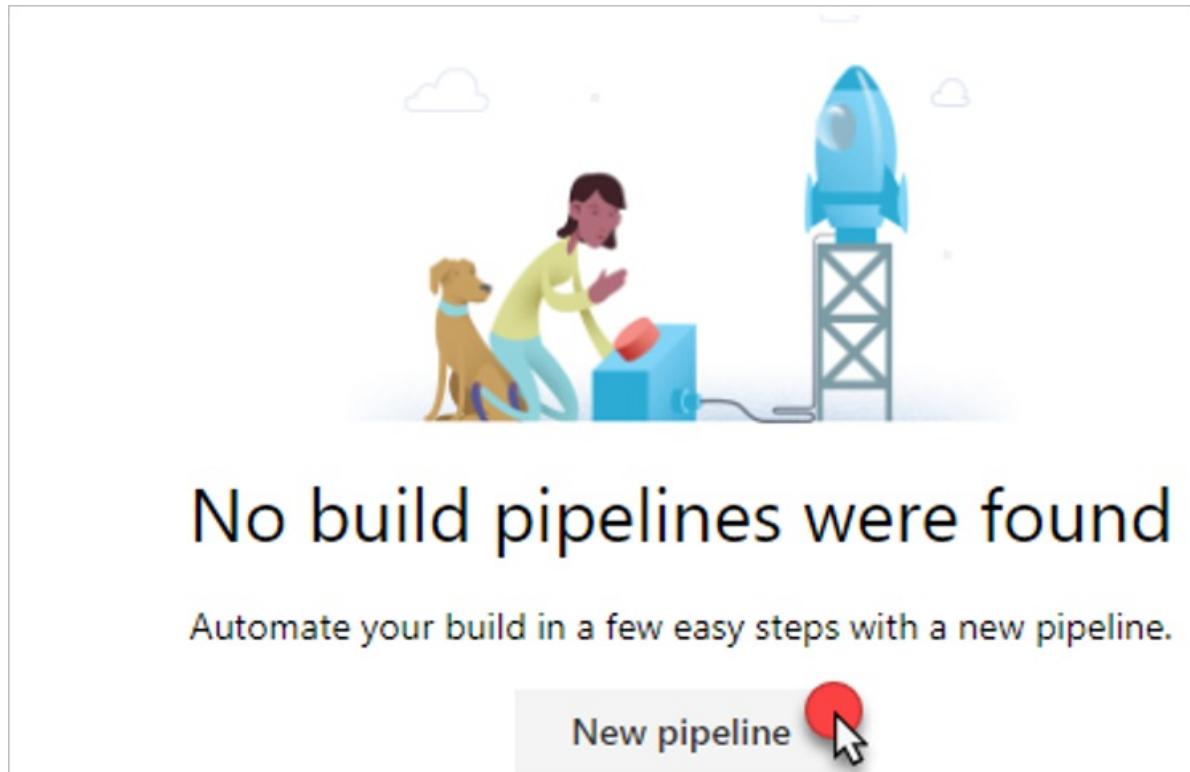
```
<client>
  <endpoint address="http://shwcf-eus2.azurewebsites.net/service.svc" binding="basicHttpBinding"
    bindingConfiguration="BasicHttpBinding_IService" contract="Data.IService"
    name="BasicHttpBinding_IService" />
</client>
```

5. With the code changes now in place, the admins commit and sync them by using Team Explorer in Visual Studio.

## Step 6: Set up build and release pipelines in Azure DevOps

The Contoso admins now configure Azure DevOps to perform the build and release process.

1. In Azure DevOps, they select **Build and release > New pipeline**.



2. They select **Azure Repos Git** and, in the **Repository** drop-down list, they select the relevant repo.

Select a source

Azure Repos Git GitHub GitHub Enterprise Subversion Bi

Team project

ContosoSmartHotel360Refactor

Repository

ContosoSmartHotel360Refactor

Default branch for manual and scheduled builds

master

Continue

- Under Select a template, they select the ASP.NET template for their build.

## Select a template

Or start with an [Empty process](#)

### Featured

ASP.NET

Build and test an ASP.NET web application.

- They use the name **ContosoSmartHotelRefactor-ASP.NET-CI** for the build and then select **Save & queue**, which kicks off the first build.



...

&gt; ContosoSmartHotelRefactor-ASP.NET-CI

Tasks

Variables

Triggers

Options

Retention

History



Save &amp; queue

5. They select the build number to watch the process. After it's finished, the admins can see the process feedback, and they select **Artifacts** to review the build results.

The screenshot shows the Azure DevOps build pipeline interface for the 'ContosoSmartHotel360Refactor-ASP.NET-CI' pipeline. At the top, there is a green circular icon with a white checkmark. To its right, the pipeline name is displayed. Below the pipeline name, there is a link to the repository ('ContosoSmartHotel360Refactor') and branch ('master'), followed by a commit hash ('6cf4413 : Deleted Containerizing the ...'). A button labeled 'Add a tag' is also present. At the bottom of the pipeline card, there is a navigation bar with several tabs: 'Logs', 'Summary', 'Tests', 'Artifacts' (which is highlighted with a red box), 'Release', 'Edit', 'Queue', and '...'. The 'Artifacts' tab is currently active, indicating that the user has selected it to review the build results.

The **Artifacts explorer** pane opens, and the **drop** folder displays the build results.

- The two .zip files are the packages that contain the applications.
- These .zip files are used in the release pipeline for deployment to Azure App Service.

# Artifacts explorer

The screenshot shows the 'drop' folder containing several deployment artifacts:

- SmartHotel.Registration.Wcf.deploy-readme.txt
- SmartHotel.Registration.Wcf.deploy.cmd
- SmartHotel.Registration.Wcf.SetParameters.xml
- SmartHotel.Registration.Wcf.SourceManifest.xml
- SmartHotel.Registration.Wcf.zip (highlighted with a red box)
- SmartHotel.Registration.Web.deploy-readme.txt
- SmartHotel.Registration.Web.deploy.cmd
- SmartHotel.Registration.Web.SetParameters.xml
- SmartHotel.Registration.Web.SourceManifest.xml
- SmartHotel.Registration.Web.zip (highlighted with a red box)

- They select Releases > + New pipeline.

The screenshot shows the 'Releases' page in Azure DevOps:

contososmarthotel360 / ContosoSmartHotel360Refa... / Pipelines / Releases

Release Management helps you automate the deployment and testing of your software in multiple stages. You can either fully automate the delivery of your software all the way to production, or set up semi-automated pipelines with approvals and on-demand deployments.

Start by creating a new release pipeline.

+ New pipeline (highlighted with a red circle)

Getting started Security

- They select the deployment template for Azure App Service.

## Select a template

Or start with an  [Empty process](#)

### Featured



#### Azure App Service deployment

Deploy your application to Azure App Service Web App on Windows, Linux, containers, Functions, and WebJobs.

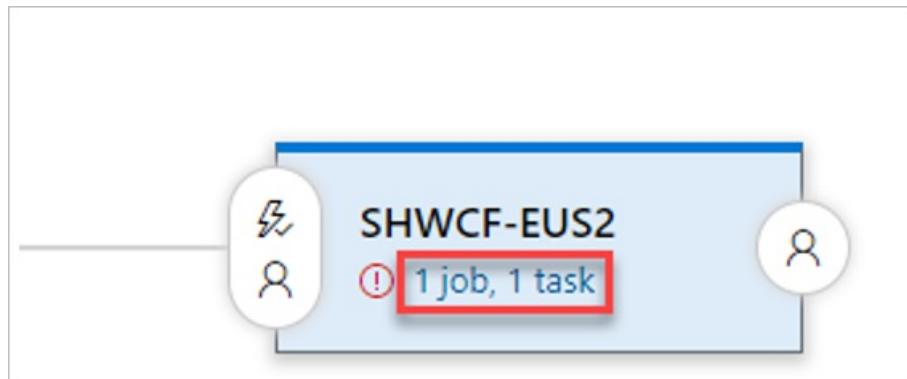
8. They name the release pipeline **ContosoSmartHotel360Refactor** and, in the **Stage name** box, specify **SHWCF-EUS2** as the name of the WCF web app.

Stage  
SHWCF-EUS2

 Properties ^  
Name and owners of the stage

Stage name

9. Under the stages, they select **1 job, 1 task** to configure deployment of the WCF service.



10. They verify that the subscription is selected and authorized, and then they select the **app service name**.

Stage name

SHWCF-EUS2

Parameters ⓘ | ⚙️ Unlink all

Azure subscription \* ⚙️ | Manage ↗

ⓘ Scoped to subscription 'Microsoft Azure Sponsorship'  
This field is linked to 1 setting in 'Deploy Azure App Service'

App type ⚙️

Web App

App service name \* ⚙️

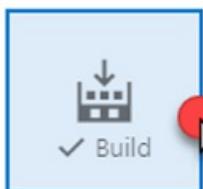
SHWCF-EUS2

This field is linked to 1 setting in 'Deploy Azure App Service'

11. On the pipeline > Artifacts, they select + Add an artifact, then select to build with the ContosoSmarthotel360Refactor pipeline.

## Add an artifact

Source type



Azure Repos ...



Github



Team Found...

4 more artifact types ▾

Project \* ⓘ

ContosoSmartHotel360Refactor

Source (build pipeline) \* ⓘ

ContosoSmartHotel360Refactor-ASP.NET-CI

Default version \* ⓘ

Latest

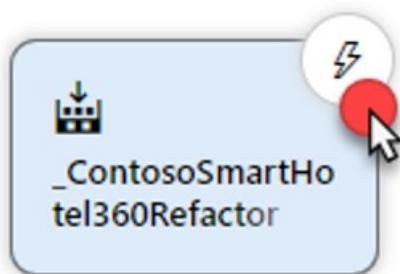
Source alias ⓘ

\_ContosoSmartHotel360Refactor-ASP.NET-CI

ⓘ The artifacts published by each version will be available for deployment in release pipelines. The latest successful build of ContosoSmartHotel360Refactor-ASP.NET-CI published the following artifacts: **drop**.

Add

12. To enable the continuous deployment trigger, the admins select the lightning bolt icon on the artifact.



13. They set the continuous deployment trigger to **Enabled**.

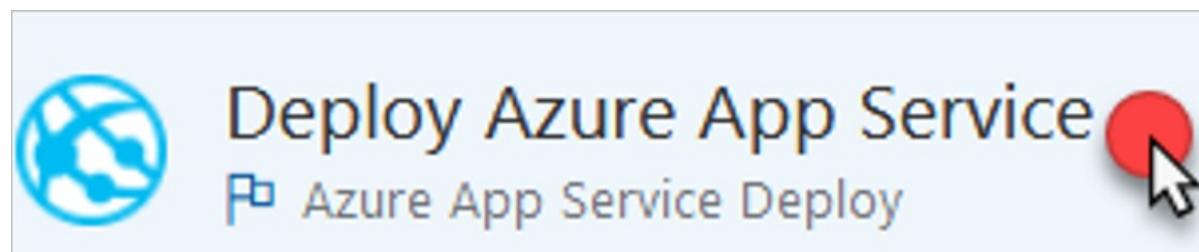
**Continuous deployment trigger**

Build: \_ContosoSmartHotel360Refactor-ASP.NET-CI

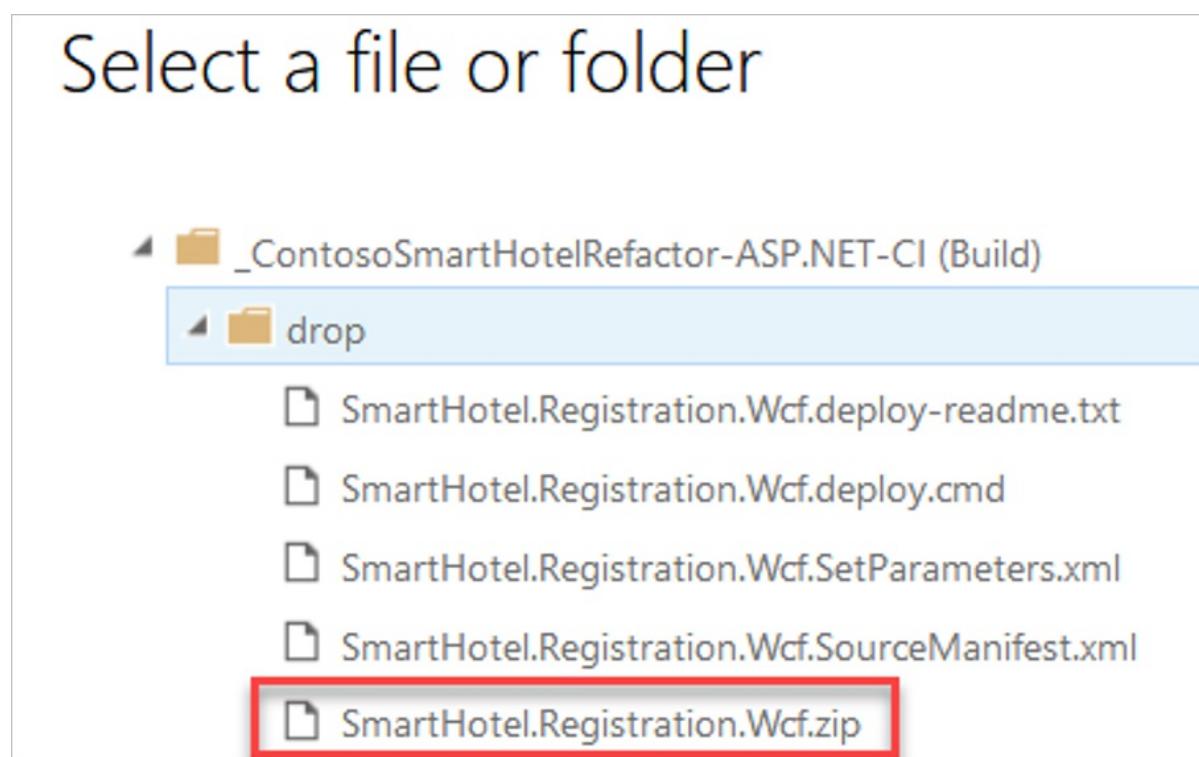
Enabled

Creates a release every time a new build is available.

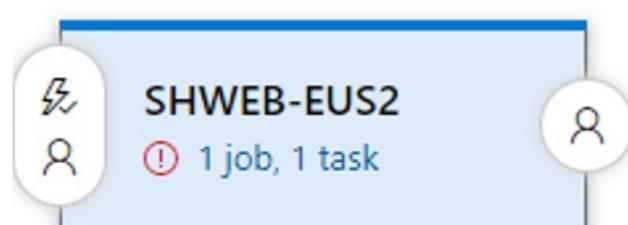
14. The admins go back to the stage 1 job, 1 task and then select Deploy Azure App Service.



15. In Select a file or folder, they expand the drop folder, select the *SmartHotel.Registration.Wcf.zip* file that was created during the build, and then select Save.



16. They select Pipeline > Stages, and then select + Add to add an environment for SHWEB-EUS2. They select another Azure App Service deployment.



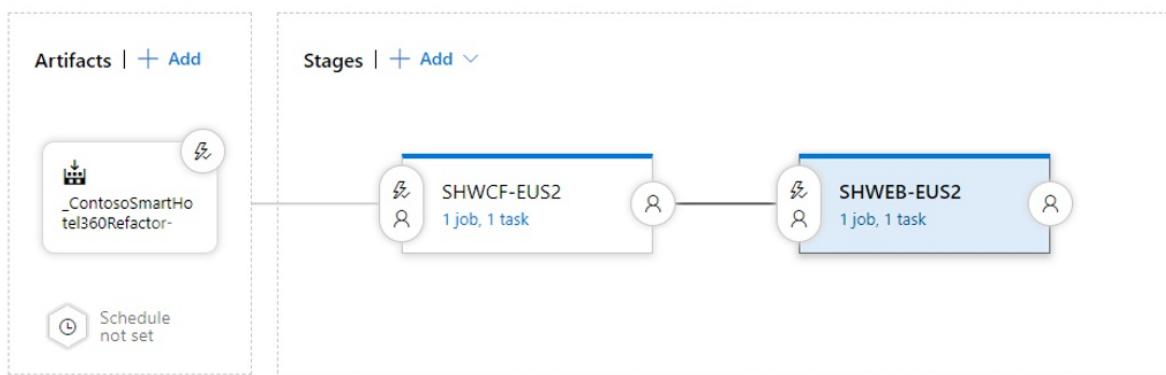
17. They repeat the process to publish the SmartHotel.Registration.Web.zip file to the correct web app, and

then select Save.

## Select a file or folder

- ▲ \_ContosoSmartHotelRefactor-ASP.NET-CI (Build)
  - ▲ drop
    - SmartHotel.Registration.Wcf.deploy-readme.txt
    - SmartHotel.Registration.Wcf.deploy.cmd
    - SmartHotel.Registration.Wcf.SetParameters.xml
    - SmartHotel.Registration.Wcf.SourceManifest.xml
    - SmartHotel.Registration.Wcf.zip
    - SmartHotel.Registration.Web.deploy-readme.txt
    - SmartHotel.Registration.Web.deploy.cmd
    - SmartHotel.Registration.Web.SetParameters.xml
    - SmartHotel.Registration.Web.SourceManifest.xml
    - **SmartHotel.Registration.Web.zip**

The release pipeline is displayed, as shown here:



18. They go back to Build, select Triggers, and then select the **Enable continuous integration** check box. This action enables the pipeline so that when changes are committed to the code, the full build and release occur.

ContosoSmartHotel360Refactor

Enable continuous integration

Batch changes while a build is in progress

Branch filters

Type	Branch specification
Include	master

+ Add

19. They select **Save & queue** to run the full pipeline. A new build is triggered, which in turn creates the first release of the application to the Azure App Service.

... > ContosoSmartHotelRefactor-ASP.NET-CI

Tasks Variables Triggers Options Retention History | **Save & queue**

20. Contoso admins can follow the build and release pipeline process from Azure DevOps. After the build finishes, the release starts.

Environments

SHWCF-EUS2 ✓ Succeeded 1 warning on 8/21/2018 7:11 PM	SHWEB-EUS2 ▷ In progress Initialize Agent 0/1 tasks 00:06
--	---

21. After the pipeline finishes, both sites have been deployed, and the application is up and running online.

Customer Name	Passport	Customer Id
Bernabè Sannicolas	587597740	Cust-101
Francesc Rispau	964981996	Cust-105
Silvestre Bolas	867400639	Cust-107

The application has been successfully migrated to Azure.

## Clean up after migration

After migration, Contoso completes these cleanup steps:

- They remove the on-premises VMs from the vCenter inventory.
- They remove the VMs from the local backup jobs.
- They update their internal documentation to show the new locations for the SmartHotel360 application. The documentation shows the database as running in Azure SQL Database and the front end as running in two web apps.
- They review any resources that interact with the decommissioned VMs, and they update any relevant settings or documentation to reflect the new configuration.

## Review the deployment

With the resources now migrated to Azure, Contoso needs to fully operationalize and help secure their new infrastructure.

### Security

- Contoso helps ensure that their new `SmartHotel-Registration` database is secure. [Learn more](#).
- In particular, Contoso updates the web apps to use SSL with certificates.

### Backups

- The Contoso team reviews the backup requirements for the Azure SQL Database. [Learn more](#).
- They also learn about managing SQL Database backups and restores. [Learn more](#) about automatic backups.
- They consider implementing failover groups to provide regional failover for the database. [Learn more](#).
- For resilience, they consider deploying the web app in the main region (`East US 2`) and the secondary region (`Central US`). The team could configure Traffic Manager to ensure failover during regional outages.

### Licensing and cost optimization

- After all resources are deployed, Contoso assigns Azure tags based on their [infrastructure planning](#).
- All licensing is built into the cost of the PaaS services that Contoso is consuming. This cost is deducted from the Enterprise Agreement.
- Contoso will use [Azure Cost Management and Billing](#) to ensure that they stay within the budgets established by their IT leadership.

## Conclusion

In this article, Contoso refactored the SmartHotel360 application in Azure by migrating the application front-end VM to two Azure App Service web apps. The application database was migrated to Azure SQL Database.

# Refactor an on-premises application to an Azure App Service web app and a SQL managed instance

11/9/2020 • 18 minutes to read • [Edit Online](#)

This article demonstrates how the fictional company Contoso refactors a two-tier Windows .NET application that's running on VMware virtual machines (VMs) as part of a migration to Azure. The Contoso team migrates the application front-end VM to an Azure App Service web app. The article also shows how Contoso migrates the application database to an Azure SQL managed instance.

The SmartHotel360 application that we use in this example is provided as open source. If you want to use it for your own testing purposes, you can download it from [GitHub](#).

## Business drivers

The Contoso IT leadership team has worked closely with business partners to understand what they want to achieve with this migration:

- **Address business growth.** Contoso is growing, and there is pressure on their on-premises systems and infrastructure.
- **Increase efficiency.** Contoso needs to remove unnecessary procedures and streamline processes for developers and users. The business needs IT to be fast and not waste time or money, thus delivering faster on customer requirements.
- **Increase agility.** Contoso IT needs to be more responsive to the needs of the business. It must be able to react faster than the changes in the marketplace, to enable success in a global economy. Reaction time must not get in the way, or become a business blocker.
- **Scale.** As the business grows successfully, Contoso IT must provide systems that are able to grow at the same pace.
- **Reduce costs.** Contoso wants to minimize licensing costs.

## Migration goals

To help determine the best migration method, the Contoso cloud team pinned down the following goals:

REQUIREMENTS	DETAILS

Requirements	Details
<b>Application</b>	<p>The application in Azure will remain as critical as it is today on-premises.</p> <p>It should have the same performance capabilities as it currently does in VMware.</p> <p>The team doesn't want to invest in the application. For now, admins will simply move the application safely to the cloud.</p> <p>The team wants to stop supporting Windows Server 2008 R2, which the application currently runs on.</p> <p>The team also wants to move away from SQL Server 2008 R2 to a modern platform as a service (PaaS) database, which will minimize the need for management.</p> <p>Contoso wants to take advantage of its investment in SQL Server licensing and Software Assurance where possible.</p> <p>In addition, Contoso wants to mitigate the single point of failure on the web tier.</p>
<b>Limitations</b>	<p>The application consists of an ASP.NET application and a Windows Communication Foundation (WCF) service running on the same VM. They want to spread these components across two web apps using the Azure App Service.</p>
<b>Azure</b>	<p>Contoso wants to move the application to Azure, but they don't want to run it on VMs. Contoso wants to use Azure PaaS services for both the web and data tiers.</p>
<b>DevOps</b>	<p>Contoso wants to move to a DevOps model that uses Azure DevOps for their builds and release pipelines.</p>

## Solution design

After pinning down their goals and requirements, Contoso designs and reviews a deployment solution. They also identify the migration process, including the Azure services that they'll use for the migration.

### Current application

- The SmartHotel360 on-premises application is tiered across two VMs, `WEBVM` and `SQLVM`.
- The VMs are located on VMware ESXi host `contosohost1.contoso.com` version 6.5.
- The VMware environment is managed by vCenter Server 6.5 (`vcenter.contoso.com`), which runs on a VM.
- Contoso has an on-premises datacenter (`contoso-datacenter`), with an on-premises domain controller (`contosodc1`).
- The on-premises VMs in the Contoso datacenter will be decommissioned after the migration is done.

### Proposed solution

- For the application web tier, Contoso has decided to use Azure App Service. This PaaS service enables them to deploy the application with just a few configuration changes. Contoso will use Visual Studio to make the change, and they'll deploy two web apps, one for the website and one for the WCF service.
- To meet requirements for a DevOps pipeline, Contoso will use Azure DevOps for source code management with Git repos. They'll use automated builds and release to build the code and deploy it to the Azure App Service.

### Database considerations

As part of the solution design process, Contoso did a feature comparison between Azure SQL Database and SQL Managed Instance. They decided to use SQL Managed Instance based on the following considerations:

- SQL Managed Instance aims to deliver almost 100 percent compatibility with the latest on-premises SQL Server version. Microsoft recommends SQL Managed Instance for customers who are running SQL Server on-premises or on infrastructure as a service (IaaS) VMs who want to migrate their applications to a fully managed service with minimal design changes.
- Contoso is planning to migrate a large number of applications from on-premises to IaaS VMs. Many of these VMs are provided by independent software vendors. Contoso realizes that using SQL Managed Instance will help ensure database compatibility for these applications. They'll use SQL Managed Instance rather than SQL Database, which might not be supported.
- Contoso can simply do a lift and shift migration to SQL Managed Instance by using the fully automated Azure Database Migration Service. With this service in place, Contoso can reuse it for future database migrations.
- SQL Managed Instance supports SQL Server Agent, an important component of the SmartHotel360 application. Contoso needs this compatibility; otherwise, they'll have to redesign the maintenance plans required by the application.
- With Software Assurance, Contoso can exchange their existing licenses for discounted rates on a SQL managed instance by using the Azure Hybrid Benefit for SQL Server. This allows Contoso to save up to 30 percent by using SQL Managed Instance.
- Their SQL managed instance is fully contained in the virtual network, so it provides greater isolation and security for Contoso's data. Contoso can get the benefits of the public cloud, while keeping the environment isolated from the public internet.
- SQL Managed Instance supports many security features, including always-encrypted, dynamic data masking, row-level security, and threat detection.

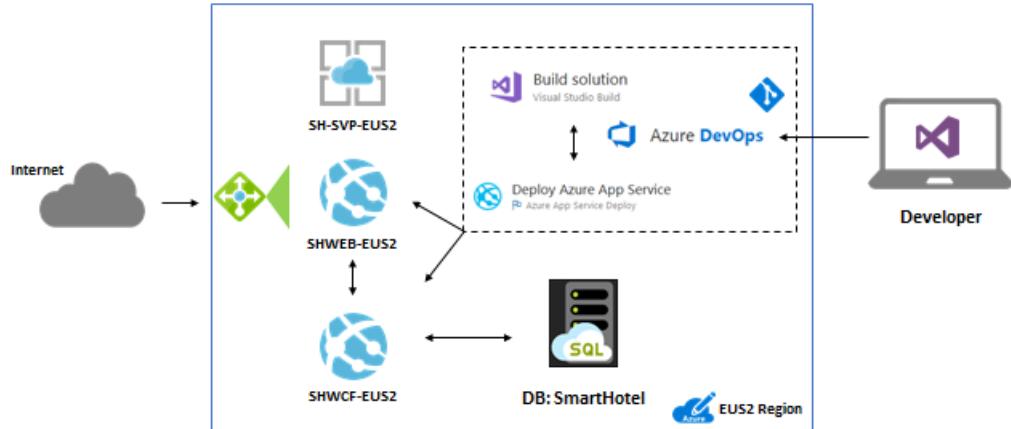
### Solution review

Contoso evaluates their proposed design by putting together a pros and cons list, as shown in the following table:

CONSIDERATION	DETAILS
---------------	---------

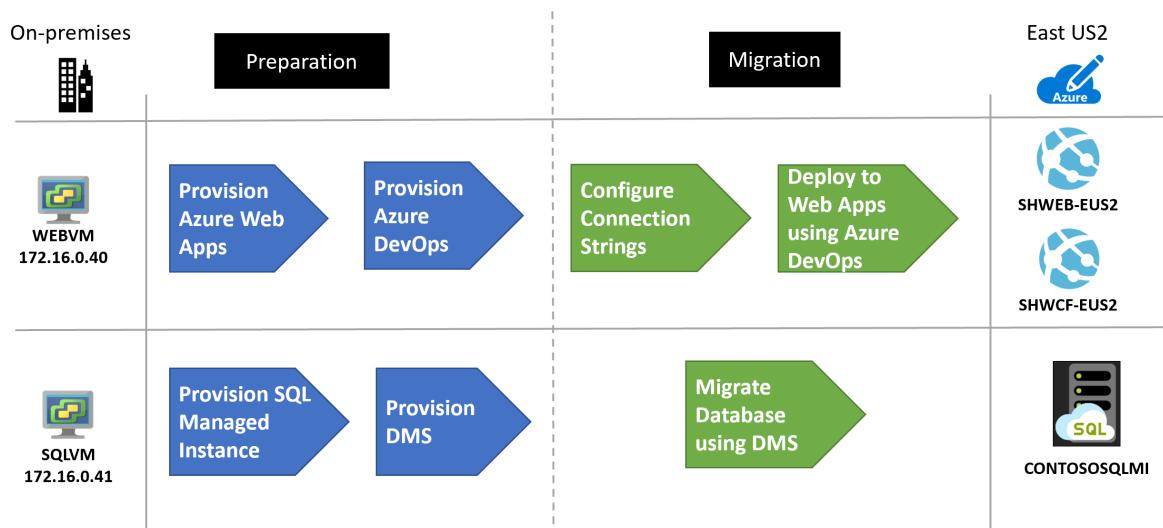
CONSIDERATION	DETAILS
Pros	<p>The SmartHotel360 application code doesn't require changes for migration to Azure.</p> <p>Contoso can take advantage of their investment in Software Assurance by using the Azure Hybrid Benefit for both SQL Server and Windows Server.</p> <p>After the migration, Windows Server 2008 R2 won't need to be supported. For more information, see the <a href="#">Microsoft Lifecycle Policy</a>.</p> <p>Contoso can configure the web tier of the application with multiple instances, so that the web tier is no longer a single point of failure.</p> <p>The database will no longer depend on the aging SQL Server 2008 R2.</p> <p>SQL Managed Instance supports Contoso's technical requirements and goals.</p> <p>Their managed instance will provide 100 percent compatibility with their current deployment, while moving them away from SQL Server 2008 R2.</p> <p>Contoso can take advantage of their investment in Software Assurance and using the Azure Hybrid Benefit for SQL Server and Windows Server.</p> <p>They can reuse Azure Database Migration Service for additional future migrations.</p> <p>Their managed instance has built-in fault tolerance that Contoso doesn't need to configure. This ensures that the data tier is no longer a single point of failover.</p>
Cons	<p>Azure App Service supports only one application deployment for each web app. This means that two web apps must be provisioned, one for the website and one for the WCF service.</p> <p>For the data tier, SQL Managed Instance might not be the best solution if Contoso wants to customize the operating system or the database server, or if they want to run third-party applications along with SQL Server. Running SQL Server on an IaaS VM could provide this flexibility.</p>

## Proposed architecture



## Migration process

1. Contoso provisions an Azure SQL managed instance and then migrates the SmartHotel360 database to it by using Azure Database Migration Service.
2. Contoso provisions and configures web apps and deploys the SmartHotel360 application to them.



## Azure services

SERVICE	DESCRIPTION	COST
Azure App Service Migration Assistant	A free and simple path to seamlessly migrate .NET web applications from on-premises to the cloud with minimal to no code changes.	It's a downloadable tool, free of charge.
Azure Database Migration Service	Azure Database Migration Service enables seamless migration from multiple database sources to Azure data platforms with minimal downtime.	Learn about <a href="#">supported regions</a> and <a href="#">Azure Database Migration Service pricing</a> .

Service	Description	Cost
Azure SQL Managed Instance	SQL Managed Instance is a managed database service that represents a fully managed SQL Server instance in Azure. It uses the same code as the latest version of SQL Server Database Engine, and has the latest features, performance improvements, and security patches.	Using a SQL managed instance that runs in Azure incurs charges based on capacity. Learn more about <a href="#">SQL Managed Instance pricing</a> .
Azure App Service	Helps create powerful cloud applications that use a fully managed platform.	Pricing is based on size, location, and usage duration. <a href="#">Learn more</a> .
Azure Pipelines	Provides a continuous integration and continuous deployment (CI/CD) pipeline for application development. The pipeline starts with a Git repository for managing application code, a build system for producing packages and other build artifacts, and a release management system to deploy changes in dev, test, and production environments.	

## Prerequisites

To run this scenario, Contoso must meet the following prerequisites:

Requirements	Details
Azure subscription	Contoso created subscriptions earlier in this article series. If you don't have an Azure subscription, create a <a href="#">free account</a> .  If you create a free account, you're the administrator of your subscription and can perform all actions.  If you use an existing subscription and you're not the administrator, you need to work with the admin to assign you Owner or Contributor permissions.
Azure infrastructure	Contoso set up their Azure infrastructure as described in <a href="#">Azure infrastructure for migration</a> .

## Scenario steps

Here's how Contoso will run the migration:

- **Step 1: Assess and migrate the web apps.** Contoso uses the [Azure App Service Migration Assistant](#) tool to run pre-migration compatibility checks and migrate their web apps to Azure App Service.
- **Step 2: Set up a SQL managed instance.** Contoso needs an existing managed instance to which the on-premises SQL Server database will migrate.
- **Step 3: Migrate via Azure Database Migration Service.** Contoso migrates the application database via Azure Database Migration Service.
- **Step 4: Set up Azure DevOps.** Contoso creates a new Azure DevOps project, and imports the Git repo.
- **Step 5: Configure connection strings.** Contoso configures connection strings so that the web tier web app, the WCF service web app, and the SQL managed instance can communicate.

- **Step 6: Set up build and release pipelines in Azure DevOps.** As a final step, Contoso sets up build and release pipelines in Azure DevOps to create the application. The team then deploys the pipelines to two separate web apps.

## Step 1: Assess and migrate the web apps

Contoso admins assess and migrate their web app using the [Azure App Service Migration Assistant](#) tool. They use the [Microsoft Learning Path](#) as a guide during the process. In brief, the admins perform the following actions:

- They use the Azure [App Service Migration Assessment](#) tool to evaluate any dependencies between their web apps and to determine if there are any incompatibilities between their on-premises web apps and what's supported on Azure App Service.
- They download the Azure App Service Migration Assistant and sign in to their Azure account.
- They choose a subscription, a resource group, and the website's domain name.

## Step 2: Set up a SQL managed instance

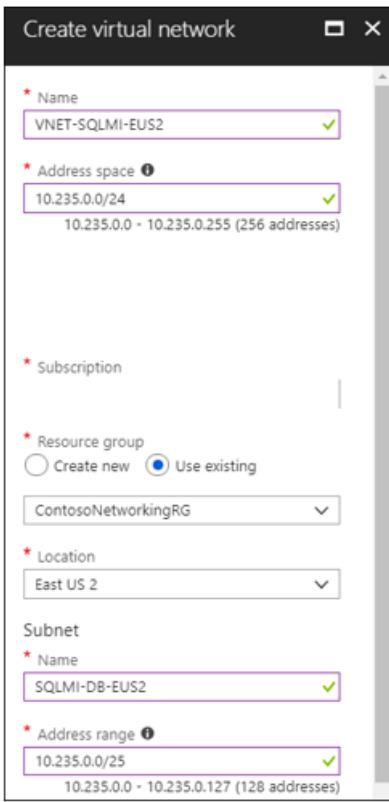
To set up an Azure SQL managed instance, Contoso needs a subnet that meets the following requirements:

- The subnet must be dedicated. It must be empty, and it can't contain any other cloud service. The subnet can't be a gateway subnet.
- After the managed instance is created, Contoso should not add resources to the subnet.
- The subnet can't have a network security group associated with it.
- The subnet must have a user-defined route table. The only route assigned should be `0.0.0.0/0` next-hop internet.
- If an optional custom DNS is specified for the virtual network, the virtual IP address `168.63.129.16` for the recursive resolvers in Azure must be added to the list. Learn how to [configure a custom DNS for an Azure SQL managed instance](#).
- The subnet must not have a service endpoint (storage or SQL) associated with it. Service endpoints should be disabled on the virtual network.
- The subnet must have a minimum of 16 IP addresses. Learn how to [size the managed instance subnet](#).
- In Contoso's hybrid environment, custom DNS settings are required. Contoso configures DNS settings to use one or more of the company's Azure DNS servers. Learn more about [DNS customization](#).

### Set up a virtual network for the managed instance

Contoso admins set up the virtual network as follows:

1. They create a new virtual network (VNET-SQLMI-EU2) in the primary region (East US 2). It adds the virtual network to the ContosoNetworkingRG resource group.
2. They assign an address space of `10.235.0.0/24`. They ensure that the range doesn't overlap with any other networks in its enterprise.
3. They add two subnets to the network:
  - `SQLMI-DS-EUS2` (`10.235.0.0/25`).
  - `SQLMI-SAW-EUS2` (`10.235.0.128/29`). This subnet is used to attach a directory to the managed instance.



4. After the virtual network and subnets are deployed, they peer networks as follows:

- Peers VNET-SQLMI-EUS2 with VNET-HUB-EUS2 (the hub virtual network for East US 2 ).
- Peers VNET-SQLMI-EUS2 with VNET-PROD-EUS2 (the production network).

NAME	PEERING STATUS	PEER
VNET-SQLMI-EUS2-to-VNET-PROD-EUS2	Connected	VNET-PROD-EUS2
VNET-SQLMI-EUS2-to-VNET-HUB-EUS2	Connected	VNET-HUB-EUS2

5. They set custom DNS settings. The DNS settings point first to Contoso's Azure domain controllers. Azure DNS is secondary. The Contoso Azure domain controllers are located as follows:

- Located in the PROD-DC-EUS2 subnet of the production network (VNET-PROD-EUS2) in the East US 2 region.
- CONTOSO DC3 address: 10.245.42.4
- CONTOSO DC4 address: 10.245.42.5
- Azure DNS resolver: 168.63.129.16

The screenshot shows the 'DNS servers' blade in the Azure portal. On the left, there's a navigation bar with links like Overview, Activity log, Access control (IAM), Tags, and Diagnose and solve problems. The main area shows the configuration for a 'Custom' DNS setup, listing three specific IP addresses. At the bottom, there's a button labeled 'Add DNS server'.

## Need more help?

- Read the [SQL Managed Instance overview](#).
- Learn how to [create a virtual network for a SQL managed instance](#).
- Learn how to [set up peering](#).
- Learn how to [update Azure Active Directory DNS settings](#).

## Set up routing

The managed instance is placed in a private virtual network. Contoso needs a route table for the virtual network to communicate with the Azure management service. If the virtual network can't communicate with the service that manages it, the virtual network becomes inaccessible.

Contoso considers these factors:

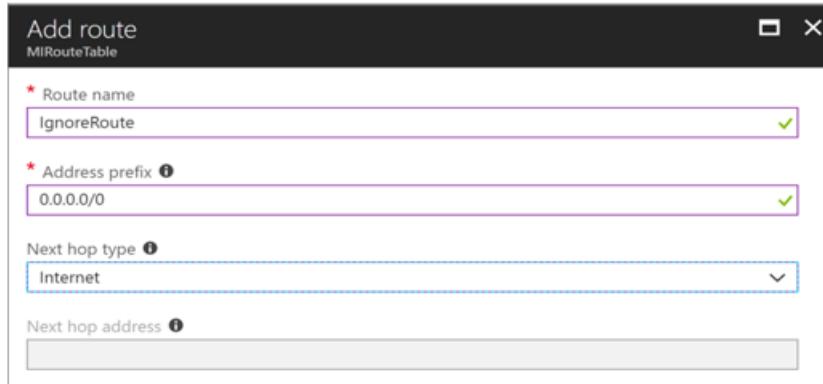
- The route table contains a set of rules (routes) that specify how packets that are sent from the managed instance should be routed in the virtual network.
- The route table is associated with subnets where managed instances are deployed. Each packet that leaves a subnet is handled based on the associated route table.
- A subnet can be associated with only one route table.
- There are no additional charges for creating route tables in Microsoft Azure.

To set up routing, Contoso admins do the following:

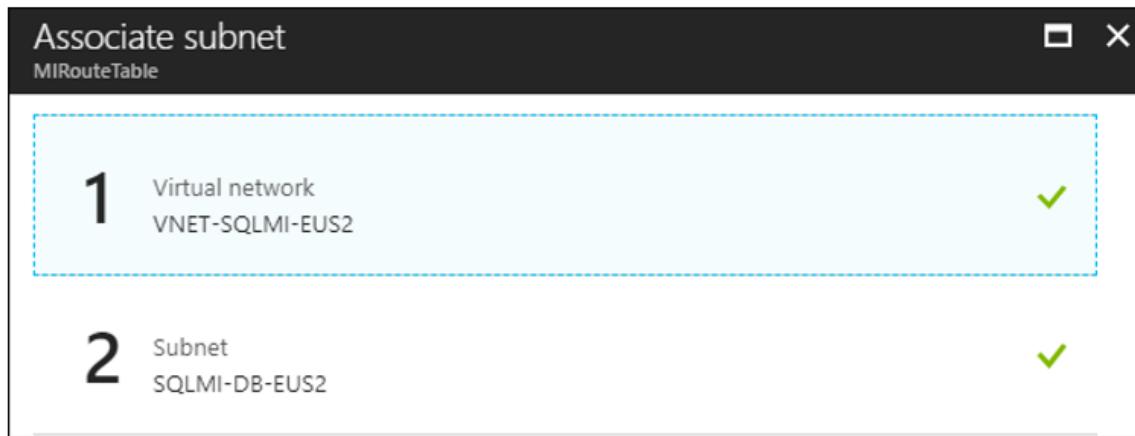
1. They create a user-defined route table in the ContosoNetworkingRG resource group.

The screenshot shows the 'Create route table' dialog. It includes fields for 'Name' (set to 'MIRouteTable'), 'Subscription' (a dropdown menu), 'Resource group' (set to 'ContosoNetworkingRG') with options to 'Create new' or 'Use existing', 'Location' (set to 'East US 2'), and a 'BGP route propagation' section with 'Disabled' and 'Enabled' buttons.

2. To comply with SQL Managed Instance requirements, after the route table (MIRouteTable) is deployed, the admins add a route with an address prefix of 0.0.0.0/0. The **Next hop type** option is set to **Internet**.



3. They associate the route table with the SQLMI-DB-EUS2 subnet (in the VNET-SQLMI-EUS2 network).



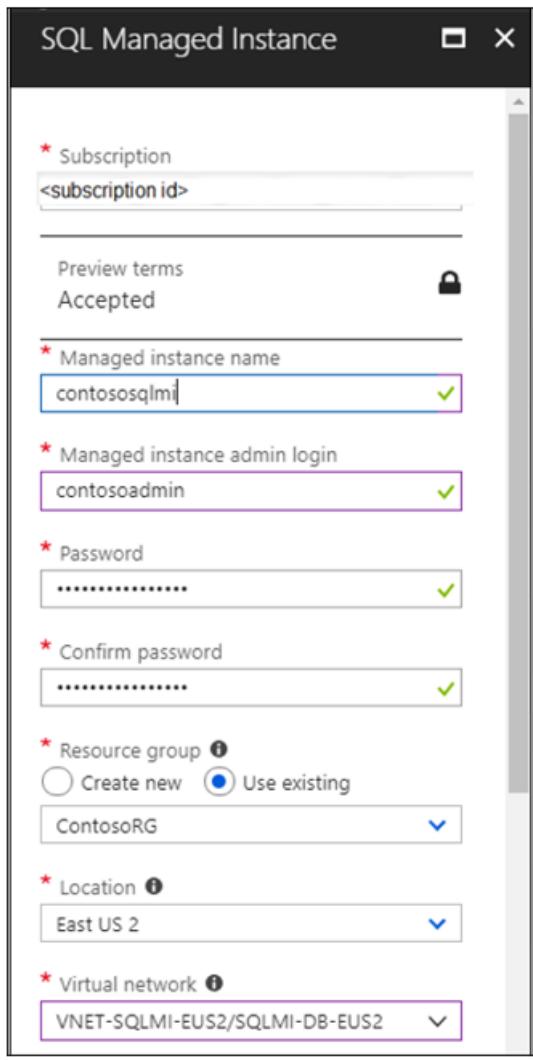
## Need more help?

Learn how to [set up routes for a managed instance](#).

## Create a managed instance

Now, Contoso admins provision a SQL managed instance by doing the following:

1. Because the managed instance serves a business application, the admins deploy the managed instance in the company's primary region (East US 2). They add the managed instance to the ContosoRG resource group.
2. They select a pricing tier, size compute, and storage for the instance. Learn more about [SQL Managed Instance pricing](#).



After the managed instance is deployed, two new resources appear in the ContosoRG resource group:

- The new SQL managed instance.
- A virtual cluster, in case Contoso has multiple managed instances.

	NAME	TYPE	LOCATION
	VirtualClusterManagedInstances	Virtual cluster	East US 2
	contososqlmi	SQL managed instance	East US 2

#### Need more help?

Learn how to [provision a managed instance](#).

## Step 3: Migrate via Azure Database Migration Service

Contoso admins migrate the managed instance via Azure Database Migration Service by following the instructions in the [step-by-step migration tutorial](#). They can perform online, offline, and hybrid (preview) migrations.

In brief, Contoso admins do the following:

- They create an Azure Database Migration Service instance with a Premium SKU that's connected to the virtual network.
- They ensure that Database Migration Service can access the remote SQL Server via the virtual network. This

would entail ensuring that all incoming ports are allowed from Azure to SQL Server at the virtual network level, the network VPN, and the machine that hosts SQL Server.

- They configure Azure Database Migration Service:
  - Create a migration project.
  - Add a source (on-premises database).
  - Select a target.
  - Select the databases to migrate.
  - Configure advanced settings.
  - Start the replication.
  - Resolve any errors.
  - Perform the final cutover.

## Step 4: Set up Azure DevOps

Contoso needs to build the DevOps infrastructure and pipelines for the application. To do this, the Contoso admins create a new DevOps project, import the code, and then set up build and release pipelines.

1. In the Contoso Azure DevOps account, they create a new project, ContosoSmartHotelRefactor, and then select **Git** for version control.

The screenshot shows the 'Create Project' dialog in the Azure DevOps interface. The 'Project name' field is filled with 'SmartHotel360Rearchitect'. The 'Description' field is empty. Under 'Visibility', there are two options: 'Public' (selected) and 'Private'. The 'Public' option is described as allowing anyone on the internet to view the project, while 'Private' is described as only allowing people you give access to view it.

<b>Project name *</b>
SmartHotel360Rearchitect
<b>Description</b>
(Empty text area)
<b>Visibility</b>
<input checked="" type="radio"/> <b>Public</b> ⓘ
Anyone on the internet can view the project. Certain features like TFVC are not supported.
<input type="radio"/> <b>Private</b>
Only people you give access to will be able to view this project.

2. They import the Git repo that currently holds their application code. They download it from the [public GitHub repository](#).

## Import a Git repository



Source type

Git



Clone URL \*

<https://github.com/Microsoft/SmartHotel360-internal-booking-apps>



Requires authorization

Import



Close

3. They connect Visual Studio to the repo and then clone the code to the developer machine by using Team Explorer.

## Connect to a Project

Showing hosted repositories for:

Add TFS Server

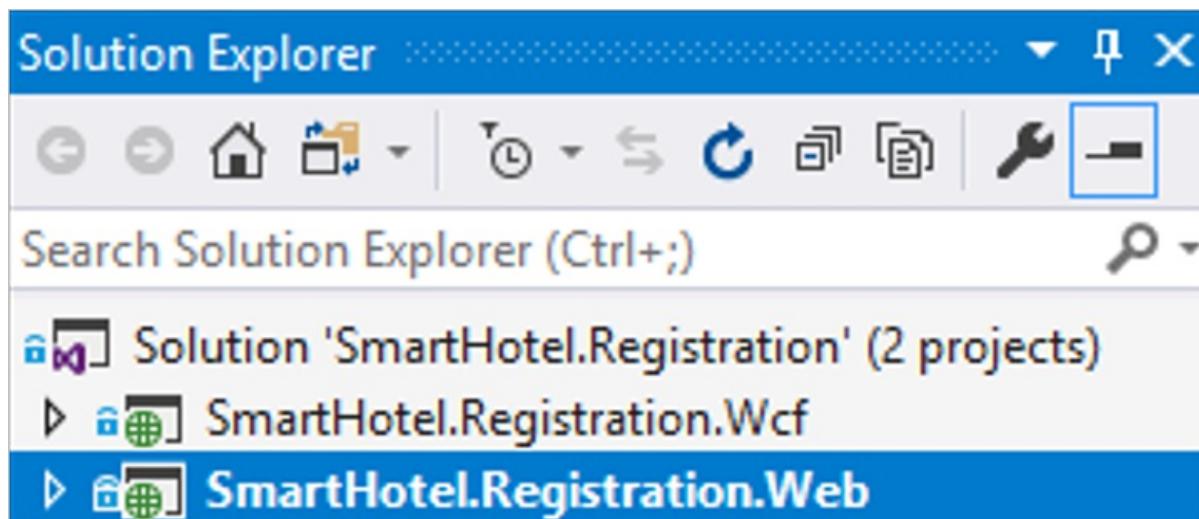
Type here to filter the list

▲ contososmarthotel360.visualstudio.com

  ▲ ContosoSmartHotel360Refactor

     ContosoSmartHotel360Refactor

4. They open the solution file for the application. The web app and WCF service have separate projects within the file.



## Step 5: Configure connection strings

The Contoso admins make sure that the web apps and database can communicate with each other. To do this, they configure connection strings in the code and in the web apps.

1. In the web app for the WCF service, SHWCF-EUS2, under **Settings > Application settings**, they add a new connection string named **DefaultConnection**.
2. They pull the connection string from the SmartHotel-Registration database and then update it with the correct credentials.

A screenshot of the Azure portal showing the "SmartHotel-Registration - Connection strings" page for a SQL database. On the left, there's a sidebar with links like Overview, Activity log, Tags, Diagnose and solve problems, Quick start, and Query editor (preview). Below that is a "SETTINGS" section with Configure, Geo-Replication, and Connection strings. The "Connection strings" link is highlighted with a red box. The main content area shows an "ADO.NET" tab selected, displaying a connection string configuration. The connection string is shown as:

```
Server=tcp:sql-smarthotel-eus2.database.windows.net,1433;Initial Catalog=SmartHotel_Web;User ID=sa;Password={your_password};MultipleActiveResultSets=False;Encrypt=True;TrustServerCertificate=False;Connection Timeout=30;
```

A red arrow points to the "Connection Timeout=30;" part of the connection string. Below the connection string, there's a link to "Download ADO.NET driver for SQL server". At the bottom of the page, there's a "Connection strings" summary table with one row for "DefaultConnection".

3. In Visual Studio, the admins open the `SmartHotel.Registration.wcf` project from the solution file. In the

project, they update the `connectionStrings` section of the `web.config` file with the connection string.

```
<connectionStrings>
  <add name="DefaultConnection" connectionString="Server=tcp:sql-smarthotel-eus2.</connectionStrings>
```

4. They change the `client` section of the `web.config` file for SmartHotel.Registration.Web to point to the new location of the WCF service. This is the URL of the WCF web app that hosts the service endpoint.

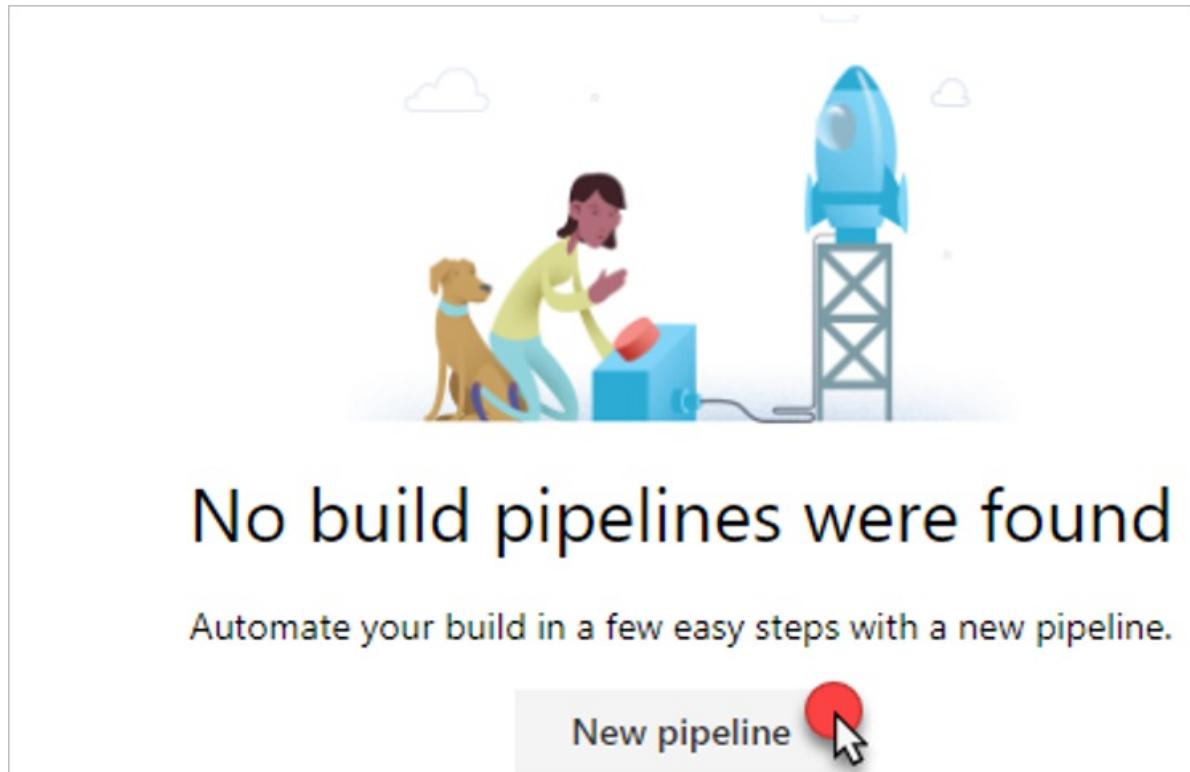
```
<client>
  <endpoint address="http://shwcf-eus2.azurewebsites.net/service.svc" binding="basicHttpBinding"
    bindingConfiguration="BasicHttpBinding_IService" contract="Data.IService"
    name="BasicHttpBinding_IService" />
</client>
```

5. With the code changes now in place, the admins commit and sync them by using Team Explorer in Visual Studio.

## Step 6: Set up build and release pipelines in Azure DevOps

The Contoso admins now configure Azure DevOps to perform the build and release process.

1. In Azure DevOps, they select **Build and release > New pipeline**.



2. They select **Azure Repos Git** and the relevant repo.

Select a source

Azure Repos Git GitHub GitHub Enterprise Subversion Bi

Team project

ContosoSmartHotel360Refactor

Repository

ContosoSmartHotel360Refactor

Default branch for manual and scheduled builds

master

Continue

3. In Select a template, they select the ASP.NET template for their build.

## Select a template

Or start with an Empty process

### Featured

ASP.NET

Build and test an ASP.NET web application.

4. They use the name ContosoSmartHotelRefactor-ASP.NET-CI for the build and then select Save & Queue, which kicks off the first build.

The screenshot shows the Azure DevOps pipeline interface for the project 'ContosoSmartHotelRefactor-ASP.NET-CI'. At the top, there are tabs for 'Tasks', 'Variables', 'Triggers', 'Options', 'Retention', and 'History'. To the right of these is a 'Save & queue' button, which is highlighted with a red box. Below the tabs, the pipeline name 'ContosoSmartHotel360Refactor-ASP.NET-CI' is displayed, along with the repository information 'ContosoSmartHotel360Refactor · master · 6cf4413 : Deleted Containerizing the ...' and a 'Add a tag' button.

5. They select the build number to watch the process. After it's finished, the admins can see the process feedback, and they select **Artifacts** to review the build results.

The screenshot shows the build results page for the pipeline 'ContosoSmartHotel360Refactor-ASP.NET-CI'. A large green circle with a white checkmark indicates the build was successful. The pipeline name is at the top, followed by the repository details 'ContosoSmartHotel360Refactor · master · 6cf4413 : Deleted Containerizing the ...' and a 'Add a tag' button. Below this is a navigation bar with tabs: 'Logs', 'Summary', 'Tests', 'Artifacts' (which is highlighted with a red box), 'Release', 'Edit', 'Queue', and '...'. The 'Artifacts' tab is currently selected, showing the build results.

The **Artifacts** explorer pane opens, and the **drop** folder displays the build results.

- The two .zip files are the packages that contain the applications.
- These .zip files are used in the release pipeline for deployment to Azure App Service.

# Artifacts explorer

The screenshot shows the 'drop' folder containing several deployment artifacts:

- SmartHotel.Registration.Wcf.deploy-readme.txt
- SmartHotel.Registration.Wcf.deploy.cmd
- SmartHotel.Registration.Wcf.SetParameters.xml
- SmartHotel.Registration.Wcf.SourceManifest.xml
- SmartHotel.Registration.Wcf.zip (highlighted with a red box)
- SmartHotel.Registration.Web.deploy-readme.txt
- SmartHotel.Registration.Web.deploy.cmd
- SmartHotel.Registration.Web.SetParameters.xml
- SmartHotel.Registration.Web.SourceManifest.xml
- SmartHotel.Registration.Web.zip (highlighted with a red box)

6. They select Releases > + New pipeline.

The screenshot shows the 'Releases' page with the following navigation:

contososmarthotel360 / ContosoSmartHotel360Refa... / Pipelines / Releases

Release Management helps you automate the deployment and testing of your software in multiple stages. You can either fully automate the delivery of your software all the way to production, or set up semi-automated pipelines with approvals and on-demand deployments.

Start by creating a new release pipeline.

+ New pipeline (button highlighted with a red circle)

Getting started Security

7. They select the deployment template for Azure App Service.

## Select a template

Or start with an  [Empty process](#)

## Featured



### Azure App Service deployment

Deploy your application to Azure App Service Web App on Windows, Linux, containers, Functions, and WebJobs.

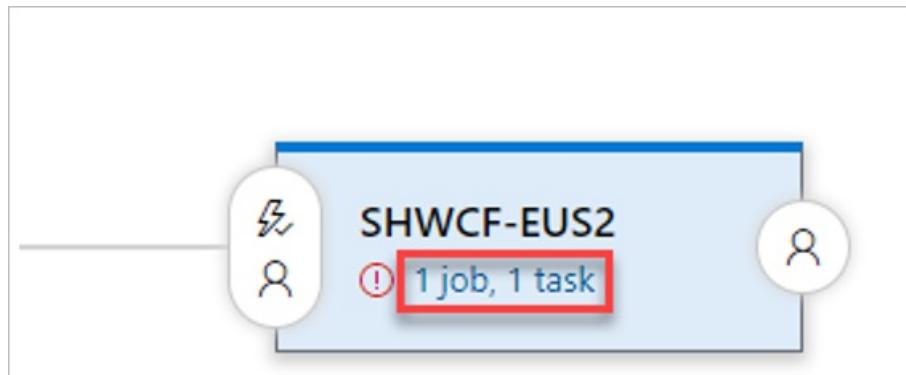
8. They name the release pipeline **ContosoSmartHotel360Refactor** and, in the **Stage name** box, specify **SHWCF-EUS2** as the name of the WCF web app.

Stage  
SHWCF-EUS2

 Properties ^  
Name and owners of the stage

Stage name

9. Under the stages, they select **1 job, 1 task** to configure deployment of the WCF service.



10. They verify that the subscription is selected and authorized, and then they select the **app service name**.

**Stage name**

SHWCF-EUS2

**Parameters** ⓘ | ⚙️ [Unlink all](#)

Azure subscription \* ⚙️ | [Manage](#) ↗

① Scoped to subscription 'Microsoft Azure Sponsorship'  
This field is linked to 1 setting in 'Deploy Azure App Service'

App type ⚙️

Web App

App service name \* ⚙️

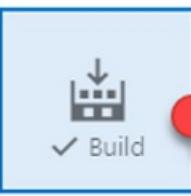
SHWCF-EUS2

This field is linked to 1 setting in 'Deploy Azure App Service'

11. On the pipeline, they select **Artifacts**, select **+ Add an artifact**, select **Build** as the source type, and then build with the `ContosoSmarthotel1360Refactor` pipeline.

## Add an artifact

Source type

 Build  Azure Repos ...  GitHub  Team Found...

[4 more artifact types ▾](#)

Project \*  ContosoSmartHotel360Refactor

Source (build pipeline) \*  ContosoSmartHotel360Refactor-ASP.NET-CI

Default version \*  Latest

Source alias  \_ContosoSmartHotel360Refactor-ASP.NET-CI

 The artifacts published by each version will be available for deployment in release pipelines. The latest successful build of **ContosoSmartHotel360Refactor-ASP.NET-CI** published the following artifacts: *drop*.

**Add**

12. To enable the continuous deployment trigger, the admins select the lightning bolt icon on the artifact.



13. They set the continuous deployment trigger to Enabled.

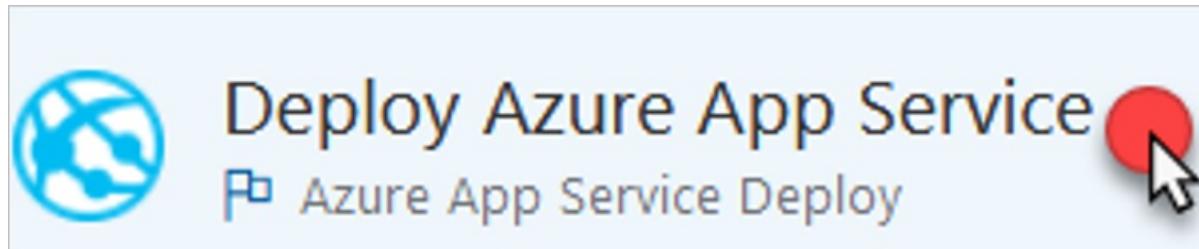
**Continuous deployment trigger**

Build: \_ContosoSmartHotel360Refactor-ASP.NET-CI

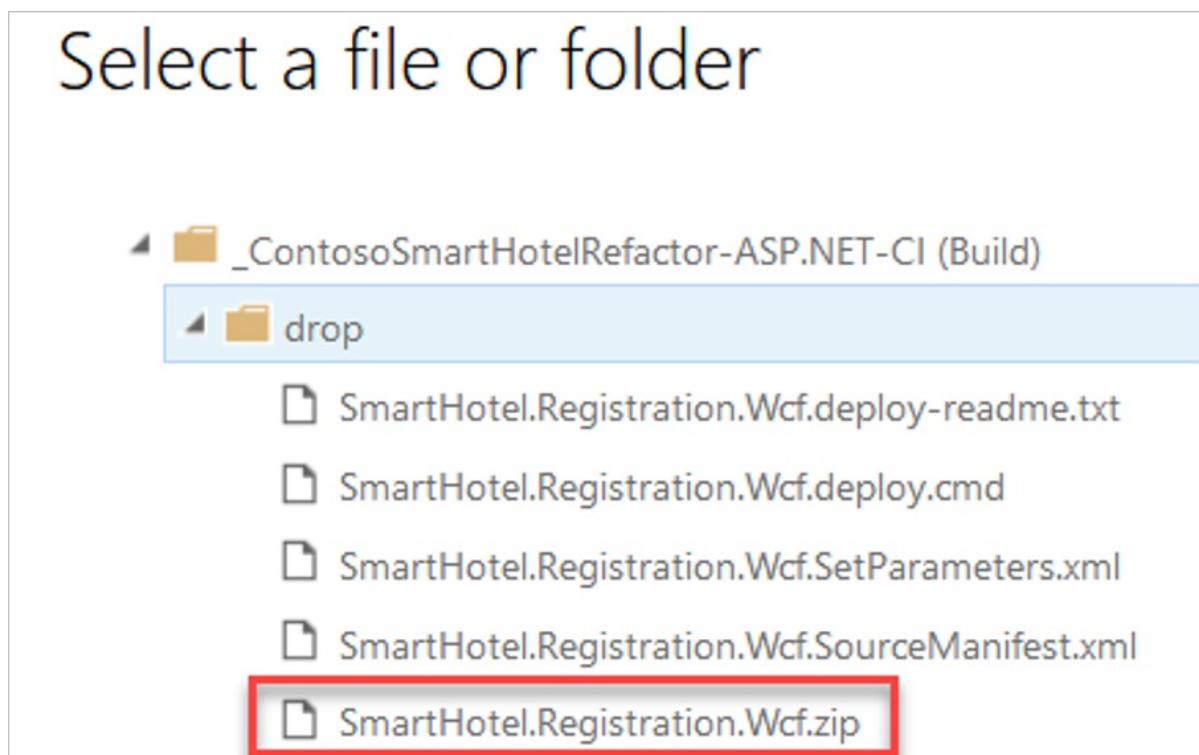
 Enabled

Creates a release every time a new build is available.

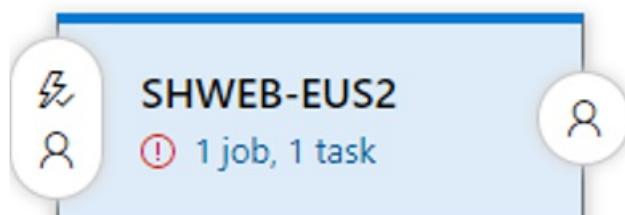
14. The admins go back to the stage 1 job, 1 task and then select Deploy Azure App Service.



15. In Select a file or folder, they expand the drop folder, select the `SmartHotel.Registration.Wcf.zip` file that was created during the build, and then select Save.



16. They select Pipeline > Stages, and then select + Add to add an environment for `SHWEB-EUS2`. They select another Azure App Service deployment.



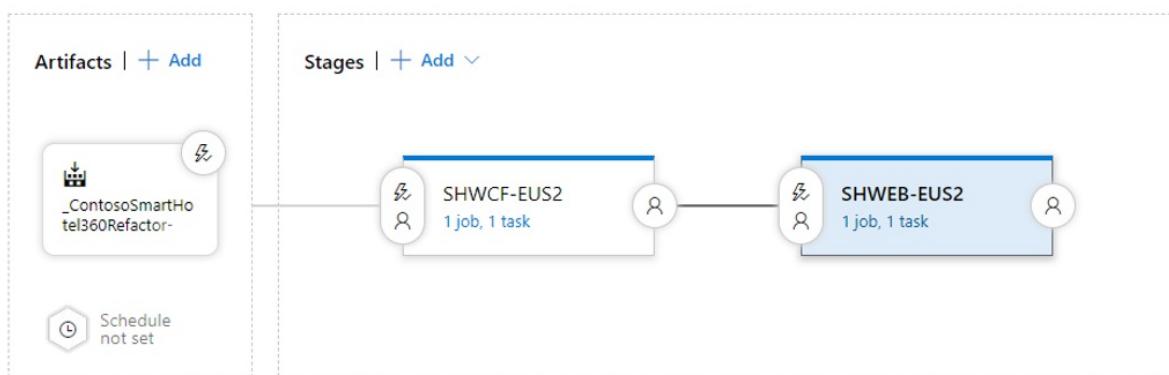
17. They repeat the process to publish the web app `SmartHotel.Registration.Web.zip` file to the correct web app,

and then select Save.

# Select a file or folder

- ◀ \_ContosoSmartHotelRefactor-ASP.NET-CI (Build)
  - ◀ drop
    - SmartHotel.Registration.Wcf.deploy-readme.txt
    - SmartHotel.Registration.Wcf.deploy.cmd
    - SmartHotel.Registration.Wcf.SetParameters.xml
    - SmartHotel.Registration.Wcf.SourceManifest.xml
    - SmartHotel.Registration.Wcf.zip
    - SmartHotel.Registration.Web.deploy-readme.txt
    - SmartHotel.Registration.Web.deploy.cmd
    - SmartHotel.Registration.Web.SetParameters.xml
    - SmartHotel.Registration.Web.SourceManifest.xml
    - **SmartHotel.Registration.Web.zip**

The release pipeline is displayed, as shown here:



18. They go back to Build, select Triggers, and then select the **Enable continuous integration** check box. This action enables the pipeline so that when changes are committed to the code, the full build and release occur.

ContosoSmartHotel360Refactor

Enable continuous integration

Batch changes while a build is in progress

Branch filters

Type	Branch specification
Include	master

+ Add

19. They select **Save & Queue** to run the full pipeline. A new build is triggered, which in turn creates the first release of the application to the Azure App Service.

... > ContosoSmartHotelRefactor-ASP.NET-CI

Tasks Variables Triggers Options Retention History | **Save & queue**

20. Contoso admins can follow the build and release pipeline process from Azure DevOps. After the build finishes, the release starts.

Environments

SHWCF-EUS2 ✓ Succeeded 1 warning on 8/21/2018 7:11 PM	SHWEB-EUS2 ▷ In progress Initialize Agent 0/1 tasks 00:06
--	---

21. After the pipeline finishes, both sites have been deployed and the application is up and running online.

Customer Name	Passport	Customer Id
Bernabè Sannicolas	587597740	Cust-101
Francesc Rispau	964981996	Cust-105
Silvestre Bolas	867400639	Cust-107

The application has been successfully migrated to Azure.

## Clean up after the migration

After the migration, the Contoso team completes the following cleanup steps:

- They remove the on-premises VMs from the vCenter inventory.
- They remove the VMs from the local backup jobs.
- They update their internal documentation to show the new locations for the SmartHotel360 application. The documentation shows the database as running in the SQL managed instance, and the front end as running in two web apps.
- They review any resources that interact with the decommissioned VMs, and they update any relevant settings or documentation to reflect the new configuration.

## Review the deployment

With the resources now migrated to Azure, Contoso needs to fully operationalize and help secure their new infrastructure.

### Security

- Contoso helps ensure that their new `SmartHotel-Registration` database is secure. [Learn more](#).
- In particular, Contoso updates the web apps to use SSL with certificates.

### Backups

- The Contoso team reviews the backup requirements for the database in Azure SQL Managed Instance. [Learn more](#).
- They also learn about managing SQL Database backups and restores. [Learn more](#) about automatic backups.
- They consider implementing failover groups to provide regional failover for the database. [Learn more](#).
- They consider deploying the web app in the main region (`East US 2`) and the secondary region (`Central US`) for resilience. The team could configure Traffic Manager to ensure failover during regional outages.

## Licensing and cost optimization

- After all resources are deployed, Contoso assigns Azure tags based on their [infrastructure planning](#).
- All licensing is built into the cost of the PaaS services that Contoso is consuming. This cost is deducted from the Enterprise Agreement.
- Contoso will use [Azure Cost Management and Billing](#) to ensure that they stay within the budgets established by their IT leadership.

## Conclusion

In this article, Contoso refactored the SmartHotel360 application in Azure by migrating the application front-end VM to two Azure App Service web apps. The application database was migrated to an Azure SQL managed instance.

# Refactor a Linux application by using Azure App Service, Traffic Manager, and Azure Database for MySQL

11/9/2020 • 14 minutes to read • [Edit Online](#)

This article shows how the fictional company Contoso refactors a two-tier [LAMP-based](#) application, migrating it from on-premises to Azure by using Azure App Service with GitHub integration and Azure Database for MySQL.

[osTicket](#), the service desk application that we use in this example, is provided as open source. If you want to use it for your own testing purposes, you can download it from the [osTicket repo in GitHub](#).

## Business drivers

The IT leadership team has worked closely with business partners to understand what they want to achieve:

- **Address business growth.** Contoso is growing and moving into new markets. It needs additional customer service agents.
- **Scale.** The solution should be built so that Contoso can add more customer service agents as the business scales.
- **Improve resiliency.** In the past, issues with the system affected internal users only. With the new business model, external users will be affected, and Contoso needs the application up and running at all times.

## Migration goals

To determine the best migration method, the Contoso cloud team has pinned down their goals for this migration:

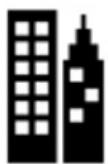
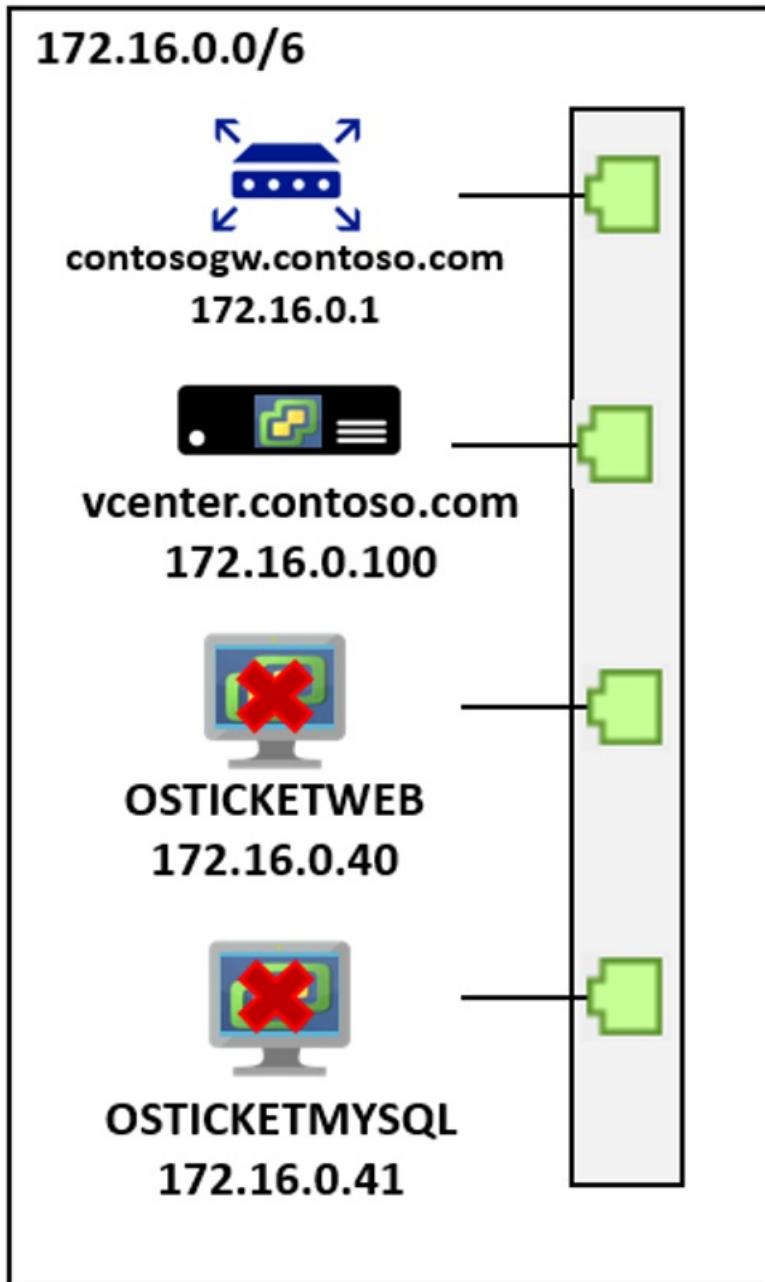
- The application should scale beyond current on-premises capacity and performance. Contoso is moving the application to take advantage of Azure's on-demand scaling.
- Contoso wants to move the application code base to a continuous delivery pipeline. As application changes are pushed to GitHub, Contoso wants to deploy those changes without tasks for operations staff.
- The application must be resilient, with capabilities for growth and failover. Contoso wants to deploy the application in two different Azure regions and set it up to scale automatically.
- Contoso wants to minimize database admin tasks after the application is moved to the cloud.

## Solution design

After pinning down their goals and requirements, Contoso designs and reviews a deployment solution, and identifies the migration process, including the Azure services that will be used for the migration.

## Current architecture

- The application is tiered across two virtual machines (VMs) (`OSTICKETWEB` and `OSTICKETMYSQL`).
- The VMs are located on VMware ESXi host `contosohost1.contoso.com` (version 6.5).
- The VMware environment is managed by vCenter Server 6.5 (`vcenter.contoso.com`), running on a VM.
- Contoso has an on-premises datacenter (`contoso-datacenter`), with an on-premises domain controller (`contosodc1`).



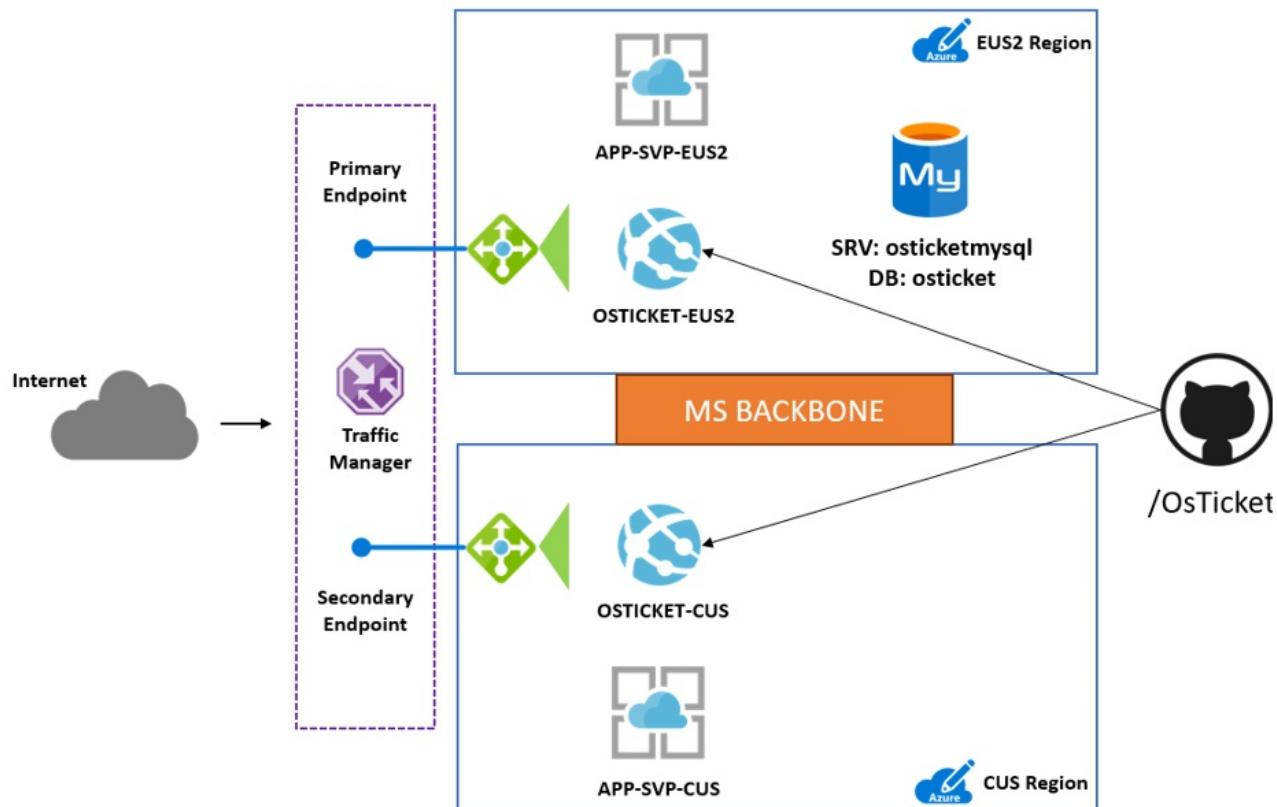
On-premises

## Proposed architecture

Here's the proposed architecture:

- The web tier application on **OSTICKETWEB** will be migrated by building an Azure App Service web app in two Azure regions. The Contoso team will implement Azure App Service for Linux by using the PHP 7.0 Docker container.
- The application code will be moved to GitHub, and the Azure App Service web app will be configured for continuous delivery with GitHub.
- Azure App Service will be deployed in both the primary region (**East US 2**) and secondary region (**Central US**).
- Azure Traffic Manager will be set up in front of the two web apps in both regions.
- Traffic Manager will be configured in priority mode to force the traffic through **East US 2**.

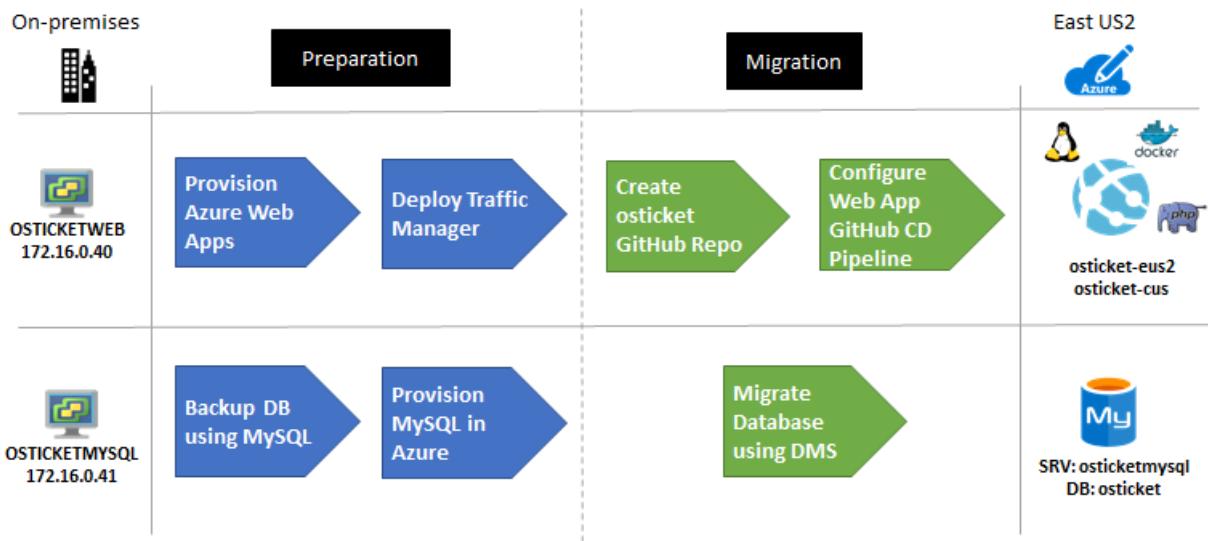
- If the Azure app server in `East US 2` goes offline, users can access the failed over application in `Central US`.
- The application database will be migrated to the Azure Database for MySQL service by using Azure Database Migration Service. The on-premises database will be backed up locally, and restored directly to Azure Database for MySQL.
- The database will reside in the primary region (`East US 2`) in the database subnet (`PROD-DB-EUS2`) of the production network (`VNET-PROD-EUS2`).
- Since they're migrating a production workload, Azure resources for the application will reside in the production resource group `ContosoORG`.
- The Traffic Manager resource will be deployed in Contoso's infrastructure resource group `ContosoInfraRG`.
- The on-premises VMs in the Contoso datacenter will be decommissioned after the migration is done.



## Migration process

Contoso completes the migration process as follows:

1. As a first step, Contoso admins set up the Azure infrastructure, including provisioning Azure App Service, setting up Traffic Manager, and provisioning an Azure Database for MySQL instance.
2. After preparing the Azure infrastructure, they migrate the database by using Azure Database Migration Service.
3. After the database is running in Azure, they upload a GitHub private repository for Azure App Service with continuous delivery, and load it with the osTicket application.
4. In the Azure portal, they load the application from GitHub to the Docker container by running Azure App Service.
5. They tweak DNS settings and configure autoscaling for the application.



## Azure services

SERVICE	DESCRIPTION	COST	
Azure App Service	The service runs and scales applications by using Azure platform as a service (PaaS) for websites.	Pricing is based on the size of the instances and the features required. <a href="#">Learn more</a> .	
Azure Traffic Manager	A load balancer that uses Domain Name System (DNS) to direct users to Azure or to external websites and services.	Pricing is based on the number of received DNS queries and the number of monitored endpoints.	<a href="#">Learn more</a> .
Azure Database Migration Service	Azure Database Migration Service enables seamless migration from multiple database sources to Azure data platforms, with minimal downtime.	Learn about <a href="#">supported regions</a> and <a href="#">Database Migration Service pricing</a> .	
Azure Database for MySQL	The database is based on the open-source MySQL database engine. It provides a fully managed, enterprise-ready community MySQL database for application development and deployment.	Pricing is based on compute, storage, and backup requirements. <a href="#">Learn more</a> .	

## Prerequisites

To run this scenario, Contoso must meet the following prerequisites:

REQUIREMENTS	DETAILS

Requirements	Details
Azure subscription	<p>Contoso created subscriptions earlier in this article series. If you don't have an Azure subscription, create a <a href="#">free account</a>.</p> <p>If you create a free account, you're the administrator of your subscription and can perform all actions.</p> <p>If you use an existing subscription and you're not the administrator, you need to work with the admin to assign you Owner or Contributor permissions.</p>
Azure infrastructure	Contoso set up their Azure infrastructure as described in <a href="#">Azure infrastructure for migration</a> .

## Scenario steps

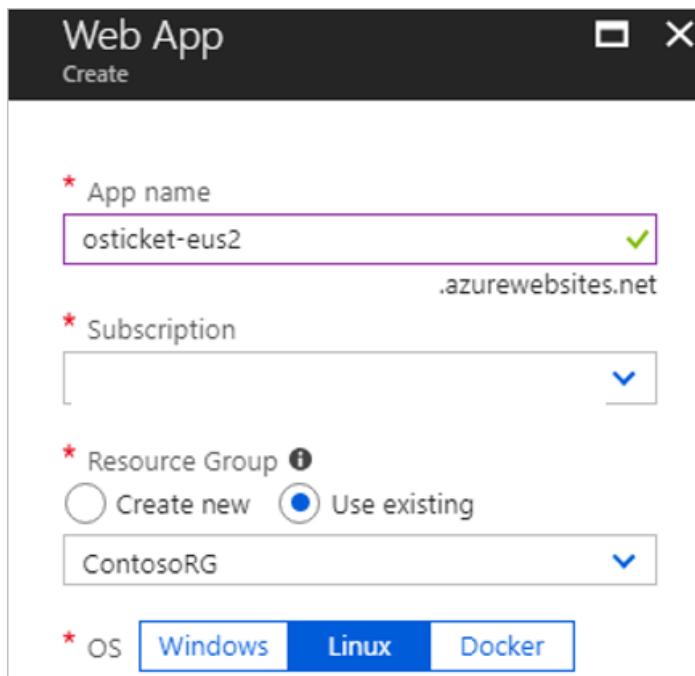
Here's the Contoso plan for completing the migration:

- **Step 1: Provision Azure App Service.** Contoso admins will provision web apps in the primary and secondary regions.
- **Step 2: Set up Traffic Manager.** They set up Traffic Manager in front of the web apps, for routing and load balancing traffic.
- **Step 3: Provision Azure Database for MySQL.** In Azure, they provision an instance of Azure Database for MySQL.
- **Step 4: Migrate the database.** They migrate the database by using Azure Database Migration Service.
- **Step 5: Set up GitHub.** They set up a local GitHub repository for the application web sites and code.
- **Step 6: Configure the web apps.** They configure the web apps with the osTicket websites.

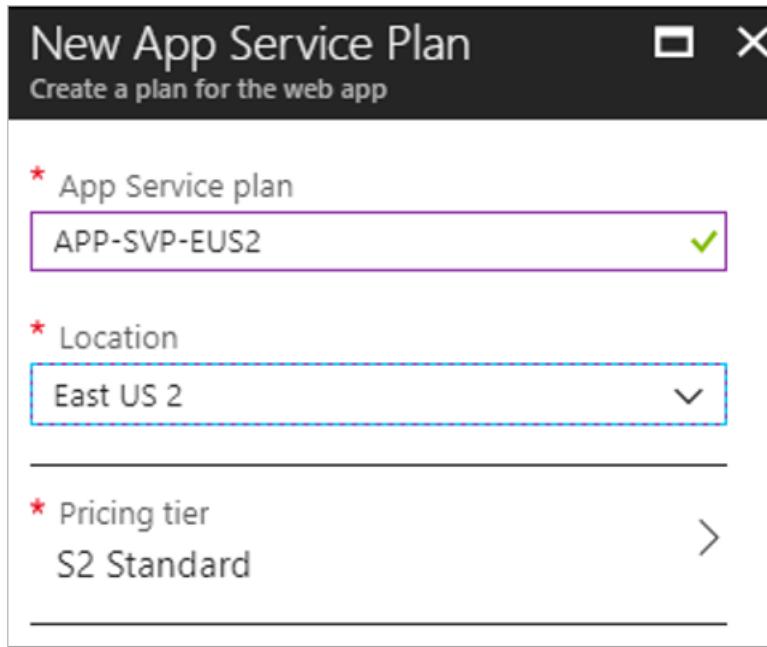
## Step 1: Provision Azure App Service

Contoso admins provision two web apps (one in each region) by using Azure App Service.

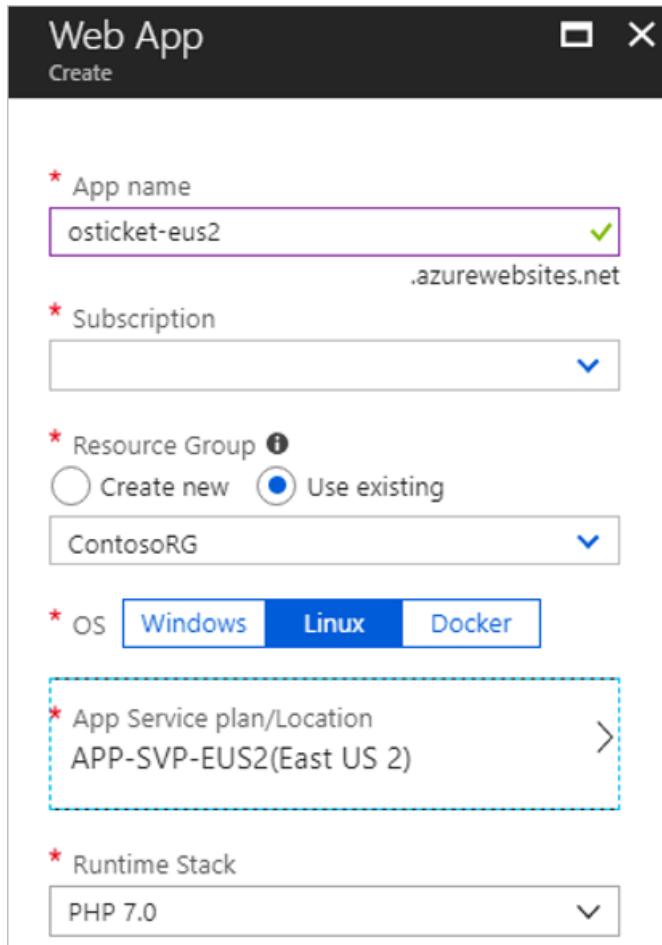
1. They create a web app resource (`osticket-eus2`) in the primary region (`East US 2`) via Azure Marketplace.
2. They put the resource in the production resource group `ContosoRG`.



3. They create an App Service plan, APP-SVP-EUS2, in the primary region, and they use the standard size.



4. They select a Linux OS with PHP 7.0 runtime stack, which is a Docker container.



5. They create a second web app, **osticket-cus**, and an Azure App Service plan for **Central US**.

**Web App**

Create

\* App name  
osticket-cus .azurewebsites.net

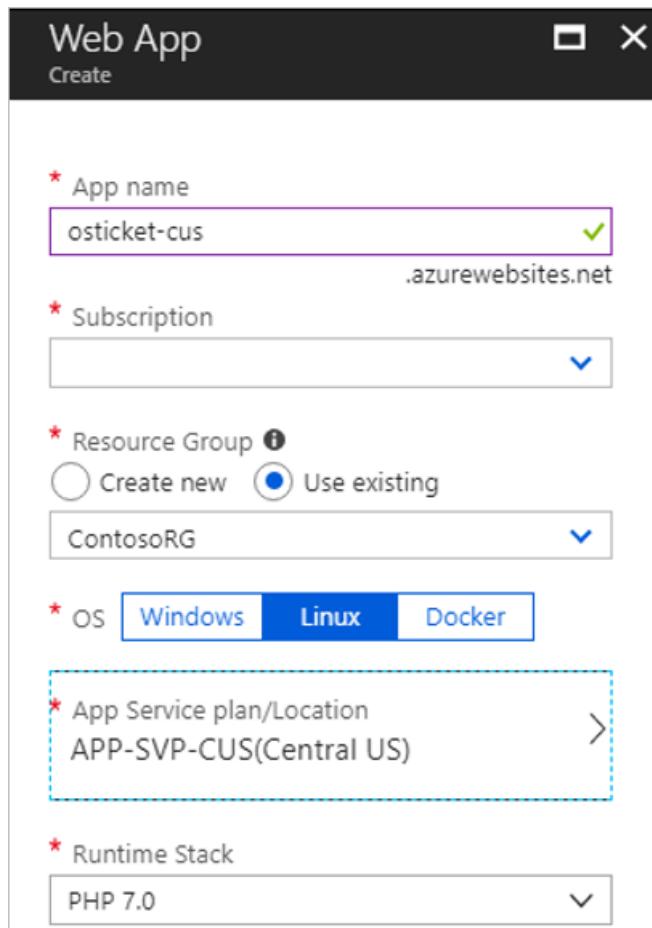
\* Subscription

\* Resource Group ⓘ  
 Create new  Use existing  
ContosoRG

\* OS **Windows** Linux Docker

\* App Service plan/Location  
APP-SVP-CUS(Central US) >

\* Runtime Stack  
PHP 7.0



Need more help?

- Learn about [Azure App Service web apps](#).
- Learn about [Azure App Service on Linux](#).

## Step 2: Set up Traffic Manager

Contoso admins set up Traffic Manager to direct inbound web requests to the web apps that are running on the osTicket web tier.

1. In Azure Marketplace, they create a Traffic Manager resource, **osticket.trafficmanager.net**. They use priority routing so that **East US 2** is the primary site. They place the resource in their existing infrastructure resource group, **ContosoInfraRG**. Note that Traffic Manager is global and not bound to a specific location.

## Create Traffic Manager profile

\* Name  
osticket ✓  
.trafficmanager.net

Routing method  
Priority

\* Subscription  
▼

\* Resource group  
 Create new  Use existing  
ContosoInfraRG

\* Resource group location ⓘ  
East US 2

2. They configure Traffic Manager with endpoints. They add the web app in East US 2 as the primary site, **osticket-eus2**, and the web app in Central US as the secondary site, **osticket-cus**.

### Add endpoint

osticket

Type ⓘ  
Azure endpoint

\* Name  
osticket-eus2 ✓

Target resource type  
App Service

\* Target resource  
osticket-eus2 >

\* Priority  
1

3. After they add the endpoints, the admins can monitor them.

NAME	STATUS	MONITOR STATUS	TYPE	PRIORITY
osticket-eus2	Enabled	Checking endpoint	Azure endpoint	1
osticket-cus	Enabled	Checking endpoint	Azure endpoint	2

Need more help?

- Learn about [Traffic Manager](#).
- Learn about [routing traffic to a priority endpoint](#).

## Step 3: Provision Azure Database for MySQL

Contoso admins provision a MySQL database instance in the primary region, East US 2.

1. In the Azure portal, they create an Azure Database for MySQL resource.

2. They add the name **contosoosticket** for the Azure database. They add the database to the production resource group **ContosoRG** and then specify credentials for it.
3. The on-premises MySQL database is version 5.7, so they select this version for compatibility. They use the default sizes, which match their database requirements.

MySQL server

contosoosticket ✓

\* Subscription <subscription id> ▾

\* Resource group ⓘ Create new  Use existing ContosoRG ▾

\* Select source Blank ▾

\* Server admin login name contosoadmin ✓

\* Password ..... ✓

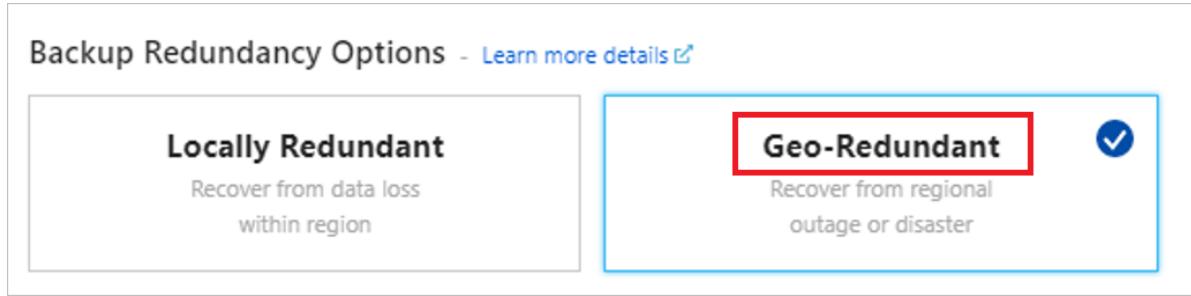
\* Confirm password ..... ✓

\* Location East US 2 ▾

\* Version 5.7 ▾

\* Pricing tier General Purpose, 2 vCore(s), 5 ... >

- For **Backup Redundancy Options**, they select **Geo-Redundant**. This option allows them to restore the database in their secondary region (Central US) if an outage occurs. They can configure this option only when they provision the database.



- They set up connection security. In the database, they select **Connection security** and then set up firewall rules to allow the database to access Azure services.
- They add the local workstation client IP address to the start and end IP addresses. This allows the web apps to access the MySQL database, along with the database client that's performing the migration.

The screenshot shows the 'Connection security' section of the Azure Database for MySQL settings. Under 'Firewall rules', there is a note about network environments. Below it, a switch labeled 'Allow access to Azure services' is turned 'ON'. A new firewall rule is listed with the name 'ClientIPAddress\_2018-4-4\_0-52-42' and an IP range of '98.249' for both start and end.

## Step 4: Migrate the database

There are several ways to move the MySQL database. Each option requires Contoso admins to create an Azure Database for MySQL instance for the target. After they create the instance, they can migrate the database by using either of two paths:

- Step 4a: Azure Database Migration Service
- Step 4b: MySQL Workbench backup and restore

### Step 4a: Migrate the database via Azure Database Migration Service

Contoso admins migrate the database via Azure Database Migration Service by following the [step-by-step migration tutorial](#). They can perform online, offline, and hybrid (preview) migrations by using MySQL 5.6 or 5.7.

#### NOTE

MySQL 8.0 is supported in Azure Database for MySQL, but the Database Migration Service tool does not yet support this version.

In brief, Contoso does the following:

- They ensure that all migration prerequisites are met:
  - The MySQL database server source must match the version that Azure Database for MySQL supports. Azure Database for MySQL supports MySQL Community Edition, the InnoDB storage engine, and migration across source and target with the same versions.
  - They enable binary logging in `my.ini` (Windows) or `my.cnf` (Unix). Failure to do this will cause the following error in the Migration Wizard:

"Error in binary logging. Variable binlog\_row\_image has value 'minimal'. Please change it to 'full'. For more information, see <https://go.microsoft.com/fwlink/?linkid=873009>."
  - The user must have the `ReplicationAdmin` role.
  - Migrate the database schemas without foreign keys and triggers.
- They create a virtual private network (VPN) that connects via ExpressRoute or VPN to the on-premises network.
- They create an Azure Database Migration Service instance with a Premium SKU that's connected to the virtual network.
- They ensure that Azure Database Migration Service can access the MySQL database via the virtual network. This entails ensuring that all incoming ports are allowed from Azure to MySQL at the virtual network level, the network VPN, and the machine that hosts MySQL.
- They run the Database Migration Service tool and then do the following:

a. Create a migration project that's based on the Premium SKU.

The screenshot shows the Azure Database Migration Service (DMS) portal. At the top, there is a navigation bar with a search bar, a 'New Migration Project' button, and other service controls like 'Delete service', 'Refresh', 'Start Service', and 'Stop Service'. Below the navigation bar, the 'Overview' section displays the status of the 'contoso-migrate' service, including its resource group ('contoso-migrate'), virtual network & IP Address ('contoso-migrate/subnets/default 172.16.0.4'), subscription ('Client Development'), and SKU ('Premium: 4 vCores'). It also shows the service's status as 'Online' and location as 'West US', with a subscription ID and service/UI version listed. A green success message at the top right says, 'Great job! Your database migration service was successfully created. You can create your first migration project now.'

The main content area is titled 'New migration project'. It contains fields for 'Project name' (set to 'MySQL') and 'Source server type \*' (set to 'MySQL'). Below these, 'Target server type \*' is set to 'Azure Database for MySQL'. A section titled 'Choose type of activity' has 'Online data migration' selected. At the bottom, a large blue button says 'Create and run activity'.

**To successfully use Database Migration Service (DMS) to migrate data, you need to:**

1. Create the target Azure Database for MySQL.
2. Deploy schema, indexes and routines to target database:
  1. Using MySQL Workbench OR
  2. Using mysqldump --no-data

b. Add a source (on-premises database).

**Migration Wizard** mysql

1 Select source >

2 Select target >

3 Select databases >

4 Configure migration settings >

5 Summary >

**Add Source Details**

Source server name  
172.16.0.41

Server port  
3306 ✓

User Name  
root

Password  
\*\*\*\*\*

TLS 1.2 security protocol  
 My server has TLS 1.2 enabled

**i** DMS requires **TLS 1.2 security protocol** enabled to establish an encrypted connection to the source MySQL database.

Follow these steps to enable TLS support:  
[TLS 1.2 support for MySQL](#)

c. Select a target.

**Migration Wizard** mysql

1 Select source ✓

2 Select target >

3 Select databases >

4 Configure migration settings >

5 Summary >

**Target details**

Target server name ⓘ  
contoso-mysql.mysql.database.azure.com

User Name  
s2admin@ contoso-mysql

Password  
\*\*\*\*\*

d. Select the databases to migrate.

The screenshot shows the 'Migration Wizard' interface with the title 'mysql'. The steps are numbered 1 through 5. Step 1 'Select source' and step 2 'Select target' are marked with green checkmarks. Step 3 'Select databases' has a grey arrow pointing right next to it. Step 4 'Configure migration settings' and step 5 'Summary' also have grey arrows pointing right. To the right of the wizard, a separate window titled 'Map to target databases' is open. It shows a search bar with 'Search' and a dropdown menu set to 'All'. Below this, it says '1 item(s)' and 'Source Database' with a checked checkbox. A 'Target Database' dropdown is shown with 'OSTICKET' selected. Navigation buttons for 'prev', 'next', and 'Page 1 of 1' are at the bottom.

e. Configure advanced settings.

The screenshot shows the 'Migration Wizard' interface with the title 'mysql'. The steps are numbered 1 through 5. Step 1 'Select source' and step 2 'Select target' are marked with green checkmarks. Step 3 'Select databases' has a grey arrow pointing right next to it. Step 4 'Configure migration settings' has a grey arrow pointing right next to it. Step 5 'Summary' has a grey arrow pointing right next to it. To the right of the wizard, a window titled 'Migration settings' is open. It shows a section for 'osticket' with an expandable 'Advanced online migration settings' section. Inside this section, there is a radio button group for 'Configure settings for large objects (LOB) data': 'Allow unlimited LOB size' (unchecked) and 'Limit LOB size' (checked). Below this is a text input field 'Limit LOB size to (KB)': '32'.

f. Start the replication and resolve any errors.

The screenshot shows the 'on-premises-one' activity details page. At the top, there are buttons for Refresh, Retry, Stop migration, Delete activity, and Download report. Below this, there are sections for 'Source server' (52.191.131.189), 'Source version' (MySQL 5.7), 'Source databases' (1), 'Type of activity' (Online), and 'Duration' (00:00:32). Under 'Activity status', it says 'Succeeded'. In the 'Migration details' table, there is one row for 'OSTICKET' with 'Status' 'Failed', 'Migration details' 'See error details', 'Duration' '00:00:02', 'Estimated application downtime' '---', and 'Finish Date' '3/20/2020, 1:25:06 PM'.

g. Perform the final cutover.

The screenshot shows the 'osticket' activity details page. At the top, there are buttons for Refresh and Start Cutover. Below this, there are sections for 'Source database name' (osticket), 'Target database name' (osticket), 'Database status' (Running), and 'Migration details' (Ready to cutover). On the right, there is a table with four columns: 'Full load completed' (15), 'Incremental updates' (0), 'Pending changes' (0), 'Full load queued' (0), 'Incremental inserts' (0), 'Applied changes' (0), 'Full load loading' (0), 'Incremental deletes' (0), and 'Tables in error state' (0). The 'Full load failed' column also shows 0.

# Complete cutover

X

When you are ready to do the migration cutover, perform the following steps to complete the database migration. Please note that the database is ready for cutover only after the full data load is completed.

1. Stop all the incoming transactions coming to the source database.
2. Wait until all the pending transactions have been applied to the target database. At that time the pending changes counter will set to 0:

Pending changes

0

Confirm

Apply

3. Reconnect your applications to the new Azure target database.

[+ New Activity](#) [Edit Project](#) [Delete project](#) [Refresh](#)

Source server : 52.191.131.189

Target server : contoso-mysql.mysql.database.azure.com

Source version : MySQL 5.7

Target version : Azure Database for MySQL 5.7

## Migration Activities (4)

Name	Activity Type	Status	Start Time
on-premises-one	Online data migration	Completed	03/20/2020, 1:24:58 PM
on-premises-one-01	Online data migration	Failed input validation	03/20/2020, 1:24:58 PM
on-premises-one-02	Online data migration	Failed input validation	03/20/2020, 1:24:58 PM
on-premises-one-03	Online data migration	Completed	03/20/2020, 1:24:58 PM

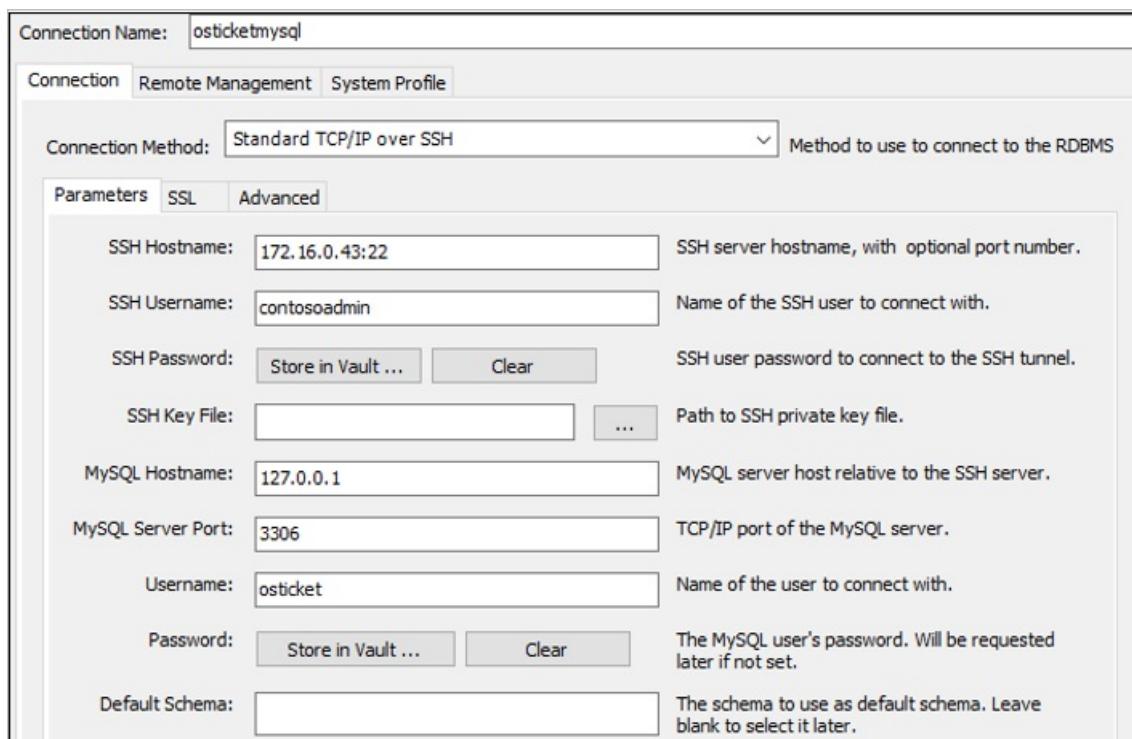
- h. Reinstate any foreign keys and triggers.
- i. Modify applications to use the new database.

- 
3. Reconnect your applications to the new Azure target database.

Completed

#### Step 4b: Migrate the database (MySQL Workbench)

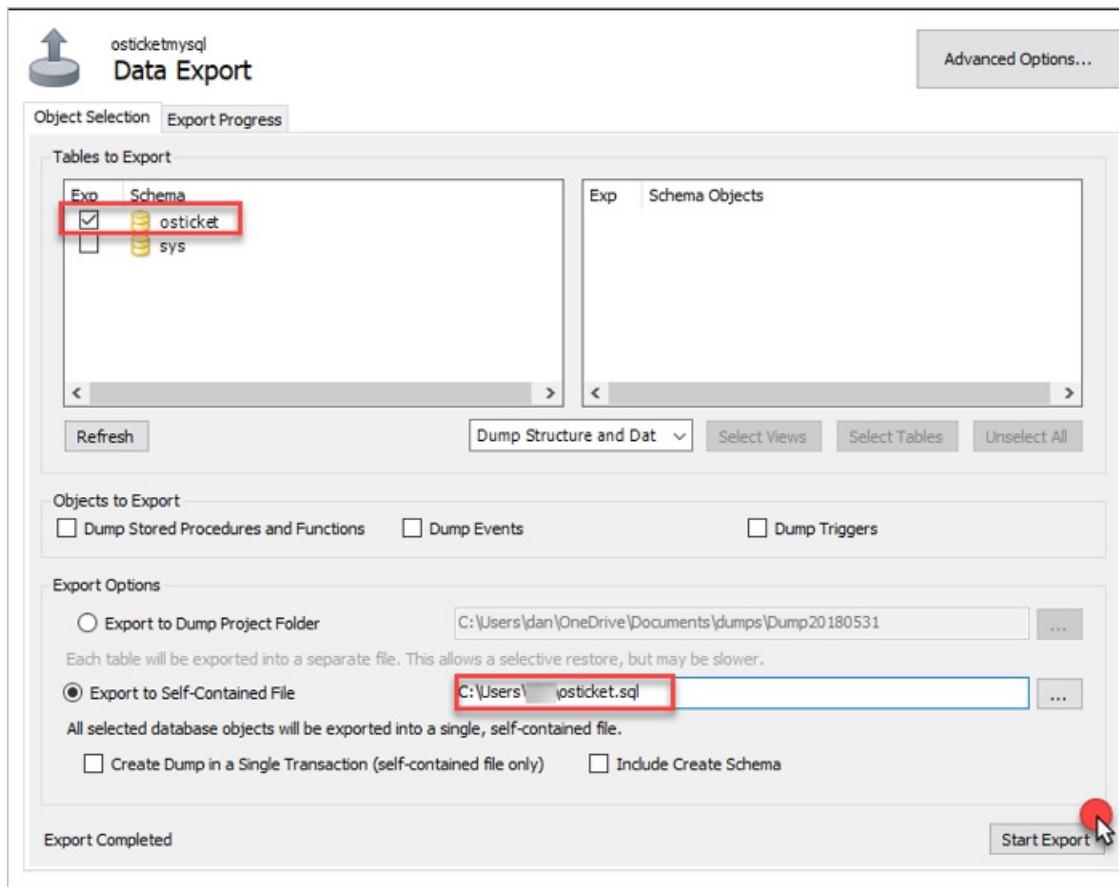
1. The Contoso admins check the [prerequisites and downloads MySQL Workbench](#).
2. They install MySQL Workbench for Windows in accordance with the [installation instructions](#). The machine that they install MySQL Workbench on must be accessible to the OSTICKETMYSQL VM and to Azure via the internet.
3. In MySQL Workbench, they create a MySQL connection to OSTICKETMYSQL.



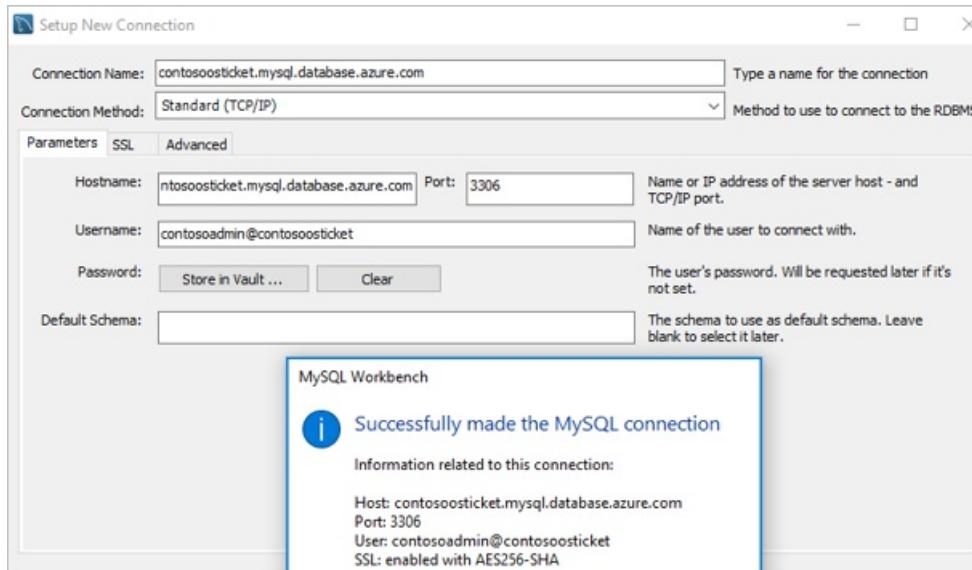
The screenshot shows the 'Connection' tab of MySQL Workbench. The 'Connection Name' is set to 'osticketmysql'. The 'Connection Method' is selected as 'Standard TCP/IP over SSH'. The 'Parameters' tab is active, displaying the following configuration:

Setting	Value	Description
SSH Hostname	172.16.0.43:22	SSH server hostname, with optional port number.
SSH Username	contosoadmin	Name of the SSH user to connect with.
SSH Password	(Store in Vault ...   Clear)	SSH user password to connect to the SSH tunnel.
SSH Key File	(Path to SSH private key file)	Path to SSH private key file.
MySQL Hostname	127.0.0.1	MySQL server host relative to the SSH server.
MySQL Server Port	3306	TCP/IP port of the MySQL server.
Username	osticket	Name of the user to connect with.
Password	(Store in Vault ...   Clear)	The MySQL user's password. Will be requested later if not set.
Default Schema	(Leave blank)	The schema to use as default schema. Leave blank to select it later.

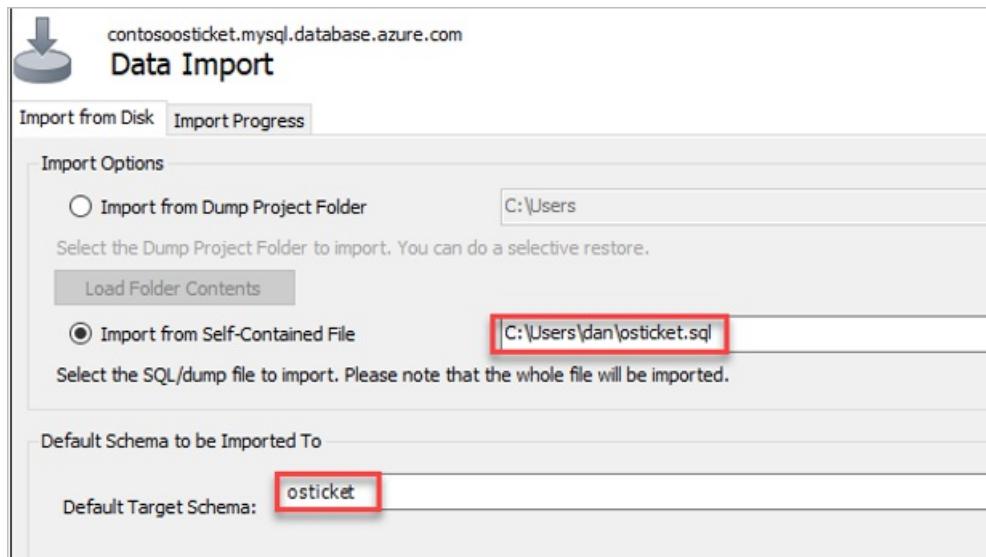
4. They export the database as `osticket` to a local self-contained file.



5. After they've backed up the database locally, the admins create a connection to the Azure Database for MySQL instance.



6. Now, they can import (restore) the database in the Azure Database for MySQL instance from the self-contained file. A new schema, `osticket`, is created for the instance.

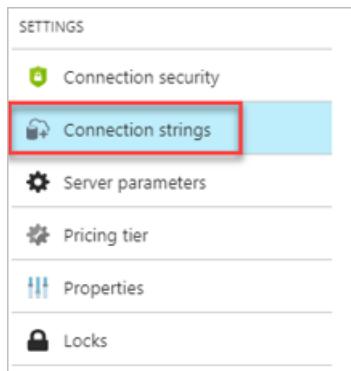


7. After they've restored the data, the admins can query it by using MySQL Workbench. The data is displayed in the Azure portal.

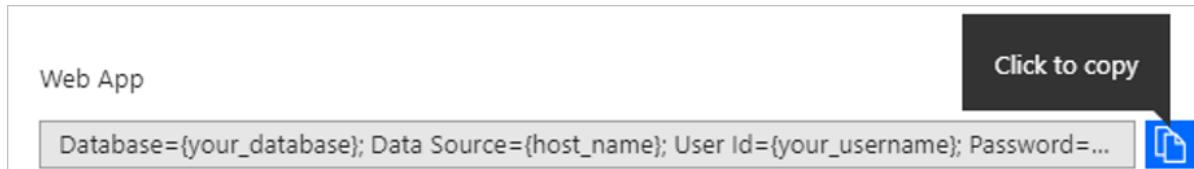
	<b>id</b>	<b>org_id</b>	<b>default_email_id</b>	<b>status</b>	<b>name</b>	<b>created</b>	<b>updated</b>
1	0	1	0	0	osTicket Support	2017-11-29 22:48:54	2017-11-29 22:48:54
2	0	2	0	0	Bill Jones	2017-11-29 22:52:23	2017-11-29 22:55:41
3	2	3	0	0	Jamal Kazmierczak	2017-11-29 22:54:31	2017-11-29 22:54:31
4	2	4	0	0	Carola Waooner	2017-11-29 22:55:00	2017-11-29 22:55:00
5	2	5	0	0	Dino Aschenbrenner	2017-11-29 22:55:27	2017-11-29 22:55:27
6	2	6	0	0	Lvn Jumper	2017-11-29 22:55:58	2017-11-29 22:55:58
7	2	7	0	0	Shayne Galbraith	2017-11-29 22:56:28	2017-11-29 22:56:28
8	2	8	0	0	Meridith Downev	2017-11-29 22:56:47	2017-11-29 22:56:47
9	2	9	0	0	Junko Chono	2017-11-29 22:57:06	2017-11-29 22:57:06
10	2	10	0	0	Van Borreson	2017-11-29 22:57:24	2017-11-29 22:57:25
11	0	11	0	0	Hailev Laber	2017-11-29 23:09:16	2017-11-29 23:09:16
12	0	12	0	0	Wavne Koop	2018-05-27 11:55:05	2018-05-27 11:55:05
13	0	13	0	0	Steve Ballmer	2018-05-27 17:09:27	2018-05-27 17:09:27
14	0	14	0	0	Wanda Somewhere	2018-05-27 17:13:33	2018-05-27 17:13:33
	<b>HULL</b>	<b>HULL</b>	<b>HULL</b>	<b>HULL</b>	<b>HULL</b>	<b>HULL</b>	<b>HULL</b>

<b>NAME</b>
information_schema
mysql
<b>osticket</b>
performance_schema
sys

8. The admins update the database information on the web apps. On the MySQL instance, they open Connection Strings.



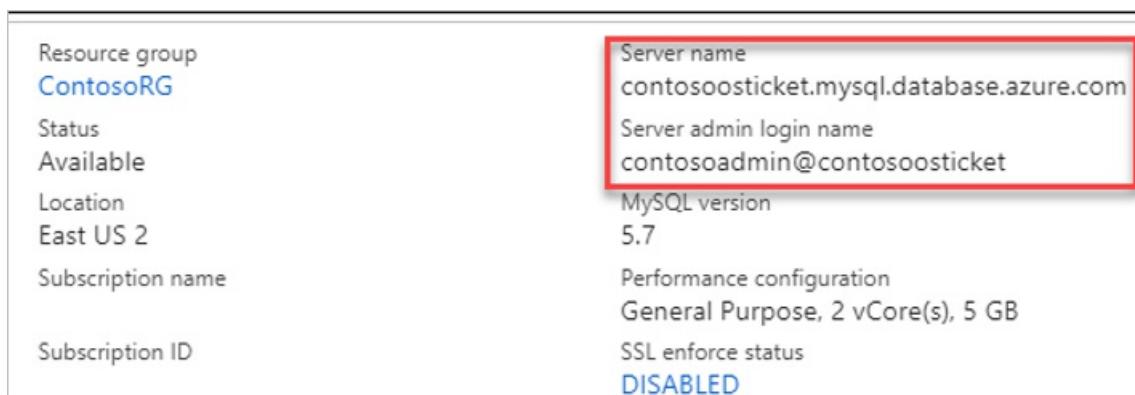
9. In the connection strings list, they select the web app settings and then copy them by selecting Click to copy.



10. They open a new file in Notepad, paste the string into it, and update the string to match the osTicket database, MySQL instance, and credentials settings.



11. They can verify the server name and login on the Overview pane in the MySQL instance in the Azure portal.



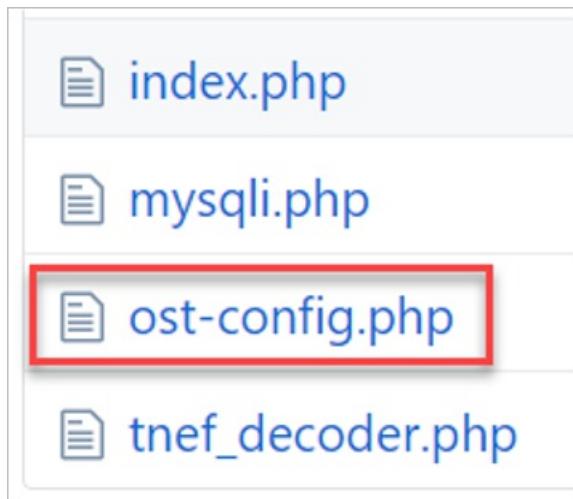
## Step 5: Set up GitHub

Contoso admins create a new private GitHub repo and set up a connection to the osTicket database in Azure Database for MySQL. Then, they load the web app into Azure App Service.

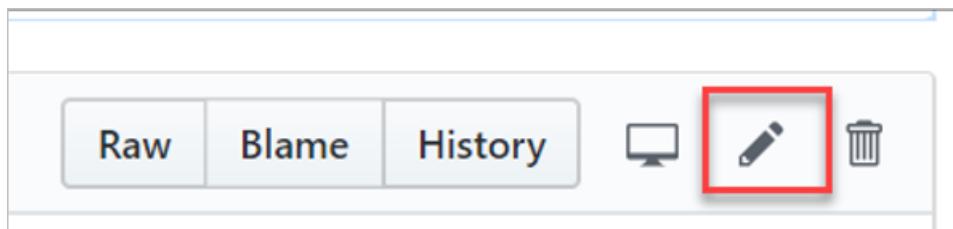
1. They browse to the osTicket software public GitHub repo and fork it to the Contoso GitHub account.



2. After they fork the repo, they go to the *include* folder and then look for and select the *ost-config.php* file.



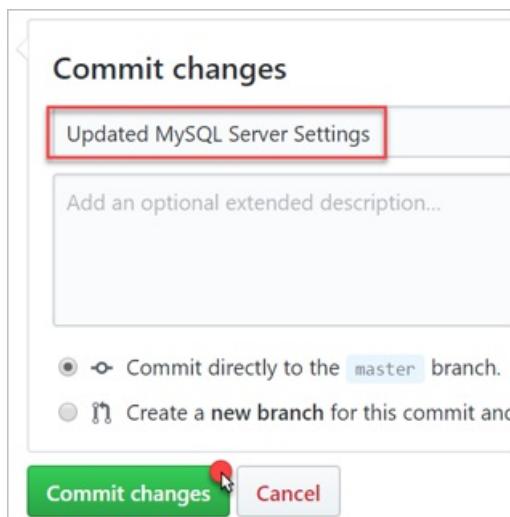
3. The file opens in the browser, and they edit it.



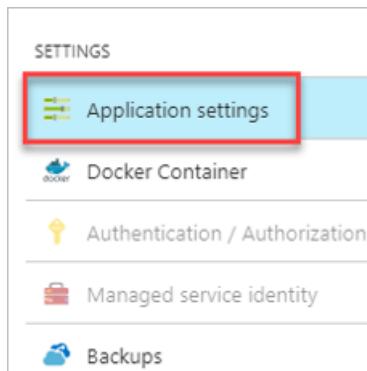
4. In the editor, the admins update the database details, specifically for DBHOST and DBUSER .

```
38 # Database Options
39 #
40 # Mysql Login info
41 define('DBTYPE','mysql');
42 define('DBHOST','contosoosticket.mysql.database.azure.com');
43 define('DBNAME','osticket');
44 define('DBUSER','contosoadmin@contosoosticket');
45 define('DBPASS','[REDACTED]');
```

5. They commit the changes.



6. For each web app (osticket-eus2 and osticket-cus), in the Azure portal, they select Application settings on the left pane and then modify the settings.



- They enter the connection string with the name `osticket`, and copy the string from Notepad into the **value area**. They select MySQL in the dropdown list next to the string, and save the settings.

A screenshot of a configuration screen showing a table of connection strings. The first row contains 'osticket' and 'Database=osticket; Data Source=osticketmysql.mys... MySQL'. The 'MySQL' part is highlighted with a red box.

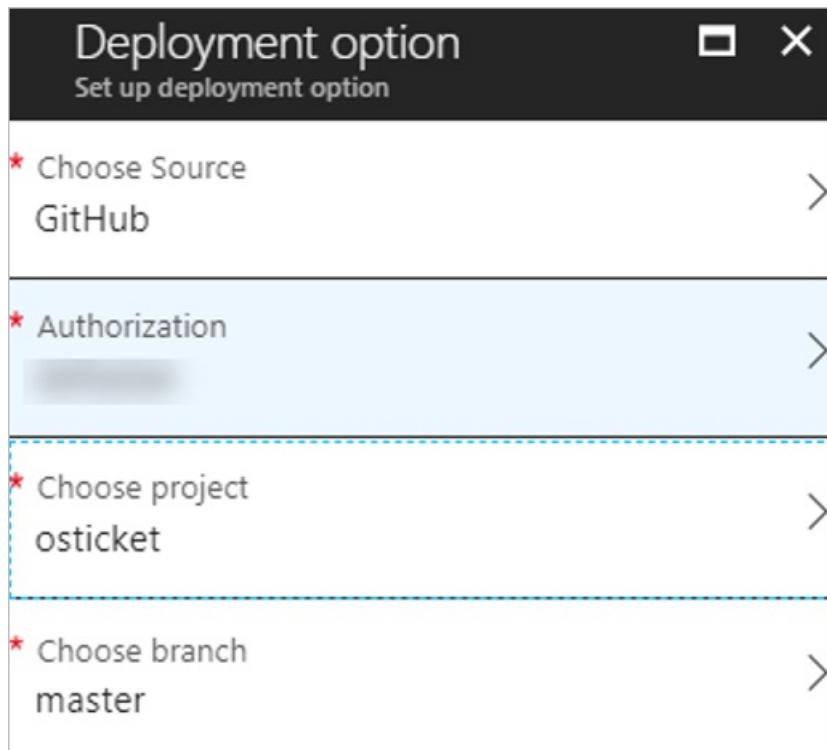
## Step 6: Configure the web apps

As the final step in the migration process, Contoso admins configure the web apps with the osTicket websites.

- In the primary web app, osticket-eus2, they open **Deployment option** and then set the source to **GitHub**.

A screenshot showing two overlapping windows. The left window is titled 'Deployment option' with a sub-section 'Choose Source'. It has a red box around the text 'Configure required settings'. The right window is titled 'Choose source' and lists three options: 'Local Git Repository By Git', 'GitHub By GitHub' (which is highlighted with a red box), and 'Bitbucket By Atlassian'.

- They select the deployment options.



3. After they set the options, the configuration shows as *Pending* in the Azure portal.

The screenshot shows the 'osticket-eus2 - Deployment options' page in the Azure portal. The 'Overview' section shows the deployment status as 'Pending'. The details pane indicates the fetch source is 'GitHub' and the status is 'Pending'.

4. After the configuration is updated and the osTicket web app is loaded from GitHub to the Docker container that runs the Azure App Service, the site shows as *Active*.

The screenshot shows the same 'osticket-eus2 - Deployment options' page after the configuration has been updated. The 'Overview' section now shows the deployment status as 'Active'. The details pane indicates the update was made to 'ost-config.php' via GitHub at 6:30 PM on Sunday, 06/03.

5. They repeat the preceding steps for the secondary web app, osticket-cus.
6. After the site is configured, it's accessible via the Traffic Manager profile. The DNS name is the new location of the osTicket application. [Learn more](#).

The screenshot shows the Azure portal interface for a Traffic Manager profile named 'osticket'. On the left, there's a navigation bar with links like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Configuration, Real user measurements, and Traffic view. The main pane is titled 'Essentials' and shows details about the resource group 'ContosoNetworkingRG', status 'Enabled', and subscription information. A table below lists endpoints: 'osticket-eus2' and 'osticket-cus', both of which are 'Enabled' and 'Online' and are categorized as 'Azure endpoint'. The 'DNS name' field is highlighted with a red box and contains the value 'http://osticket.trafficmanager.net'.

- Contoso wants to use a DNS name that's easy to remember. On the **New Resource Record** pane, they create an alias, CNAME, and a full qualified domain name, **osticket.contoso.com**, which points to the Traffic Manager name in the DNS on their domain controllers.

The screenshot shows the 'New Resource Record' dialog box. The 'Alias (CNAME)' tab is selected. In the 'Alias name (uses parent domain if left blank):' field, the value 'osticket' is entered. In the 'Fully qualified domain name (FQDN):' field, the value 'osticket.contoso.com.' is entered. In the 'Fully qualified domain name (FQDN) for target host:' field, the value 'osticket.trafficmanager.net' is entered. A 'Browse...' button is also visible next to this field.

- They configure both the osticket-eus2 and osticket-cus web apps to allow the custom host names.

The screenshot shows the 'Add hostname' dialog box for the web app 'osticket-eus2'. At the top, it says 'Add hostname' and 'osticket-eus2'. Below that, there's a section labeled '★ Hostname' with a field containing 'osticket.contoso.com' which has a green checkmark to its right. At the bottom of this section is a 'Validate' button, which is highlighted with a red circle and a cursor arrow pointing to it. Below this is a section labeled 'Hostname record type' with a dropdown menu set to 'CNAME (www.example.com or any subdomain)'.

**Set up autoscaling**

Finally, the Contoso admins set up automatic scaling for the application. Automatic scaling ensures that, as agents use the application, the application instances increase and decrease according to business needs.

1. In App Service APP-SVP-EUS2, they open Scale Unit.
2. They configure a new autoscale setting with a single rule that increases the instance count by one when the CPU usage for the current instance is above 70 percent for 10 minutes.

\* Autoscale setting name: OsTicketAutoScale

Resource group: ContosoRG

**Default** Auto created scale condition

Delete warning: The very last or default recurrence rule cannot be deleted. Instead, you can disable autoscale to turn off autoscale.

Scale mode: Scale based on a metric

Rules:

- Scale out
  - When: APP-SVP-EUS2 (Average) CpuPercentage > 70 Increase instance count by 1
  - + Add a rule

Instance limits:  
Minimum: 2  
Maximum: 10  
Default: 2

Schedule: This scale condition is executed when none of the other scale condition(s) match

3. They configure the same setting on APP-SVP-CUS to ensure that the same behavior applies if the application fails over to the secondary region. The only difference is that they set the default instance to 1, because this is for failovers only.

\* Autoscale setting name: OsTicketAutoScale-CUS

Resource group: ContosoRG

**Default** Auto created scale condition

Delete warning: The very last or default recurrence rule cannot be deleted. Instead, you can disable autoscale to turn off autoscale.

Scale mode: Scale based on a metric

Rules:

- Scale out
  - When: APP-SVP-CUS (Average) CpuPercentage > 70 Increase instance count by 1
  - + Add a rule

Instance limits:  
Minimum: 1  
Maximum: 10  
Default: 1

Schedule: This scale condition is executed when none of the other scale condition(s) match

## Clean up after migration

With the migration complete, the osTicket application is refactored to run in an Azure App Service web app with continuous delivery by using a private GitHub repo. The application runs in two regions for increased resilience. The osTicket database runs in Azure Database for MySQL after migration to the PaaS platform.

To clean up after the migration, Contoso does the following:

- They remove the VMware VMs from the vCenter inventory.
- They remove the on-premises VMs from local backup jobs.
- They update internal documentation to show new locations and IP addresses.
- They review any resources that interact with the on-premises VMs, and update any relevant settings or documentation to reflect the new configuration.
- They reconfigure monitoring to point to the `osticket-trafficmanager.net` URL, to track that the application is up and running.

## Review the deployment

With the application now running, Contoso needs to fully operationalize and secure their new infrastructure.

### Security

The Contoso security team reviews the application to determine any security issues. They identify that the communication between the osTicket application and the MySQL database instance isn't configured for SSL. They do all this to ensure that the database traffic can't be hacked. [Learn more](#).

### Backups

- The osTicket web apps don't contain state data and thus don't require backup.
- The Contoso team doesn't need to configure backup for the database. Azure Database for MySQL automatically creates server backups and stores. The team elected to use geo-redundancy for the database, so it's resilient and production-ready. Backups can be used to restore their server to a point-in-time. [Learn more](#).

### Licensing and cost optimization

- There are no licensing issues for the PaaS deployment.
- Contoso will use [Azure Cost Management and Billing](#) to ensure that they stay within the budgets established by their IT leadership.

# Rebuild an on-premises application in Azure

11/9/2020 • 23 minutes to read • [Edit Online](#)

This article demonstrates how the fictional company Contoso rebuilds a two-tier Windows .NET application that's running on VMware virtual machines (VMs) as part of a migration to Azure. Contoso migrates the front-end VM to an Azure App Service web app. Contoso builds the application back end by using microservices that are deployed to containers managed by Azure Kubernetes Service (AKS). The site interacts with Azure Functions to provide pet photo functionality.

The SmartHotel360 application used in this example is provided under an open-source license. If you want to use it for your own testing purposes, you can download it from [GitHub](#).

## Business drivers

The Contoso IT leadership team has worked closely with business partners to understand what they want to achieve with this migration:

- **Address business growth.** Contoso is growing and wants to provide differentiated experiences for customers on Contoso websites.
- **Be agile.** Contoso must be able to react faster than the changes in the marketplace to enable their success in a global economy.
- **Scale.** As the business grows successfully, the Contoso IT team must provide systems that can grow at the same pace.
- **Reduce costs.** Contoso wants to minimize licensing costs.

## Migration goals

The Contoso cloud team has pinned down application requirements for this migration. These requirements were used to determine the best migration method:

- The application in Azure must remain as critical as it is today on-premises. It should perform well and scale easily.
- The application shouldn't use infrastructure as a service (IaaS) components. Everything should be built to use platform as a service (PaaS) or serverless services.
- Application builds should run in cloud services, and containers should reside in a private, enterprise-wide registry in the cloud.
- The API service that's used for pet photos should be accurate and reliable in the real world, because decisions made by the application must be honored in their hotels. Any pet granted access is allowed to stay at the hotels.
- To meet requirements for a DevOps pipeline, Contoso will use a Git repository in Azure Repos for source code management. Automated builds and releases will be used to build code and deploy to Azure App Service, Azure Functions, and AKS.
- Separate continuous integration/continuous development (CI/CD) pipelines are needed for microservices on the back end and for the website on the front end.
- The back-end services and the front-end web app have different release cycles. To meet this requirement, Contoso will deploy two different pipelines.
- Contoso needs management approval for all front-end website deployment, and the CI/CD pipeline must provide this.

# Solution design

After pinning down their goals and requirements, Contoso designs and reviews a deployment solution, and identifies the migration process, including the Azure services that will be used for the migration.

## Current application

- The SmartHotel360 on-premises application is tiered across two VMs (WEBVM and SQLVM).
- The VMs are located on VMware ESXi host contosohost1.contoso.com (version 6.5).
- The VMware environment is managed by vCenter Server 6.5 (vcenter.contoso.com), running on a VM.
- Contoso has an on-premises datacenter (contoso-datacenter), with an on-premises domain controller (contosodc1).
- The on-premises VMs in the Contoso datacenter will be decommissioned after the migration is done.

## Proposed architecture

- The front end of the application is deployed as an Azure App Service web app in the primary Azure region.
- An Azure function provides uploads of pet photos, and the site interacts with this functionality.
- The pet photo function uses the Computer Vision API of Azure Cognitive Services along with Azure Cosmos DB.
- The back end of the site is built by using microservices. These microservices will be deployed to containers that are managed in AKS.
- Containers will be built using Azure DevOps and then pushed to Azure Container Registry.
- For now, Contoso will manually deploy the web app and function code by using Visual Studio.
- Contoso will deploy microservices by using a PowerShell script that calls Kubernetes command-line tools.

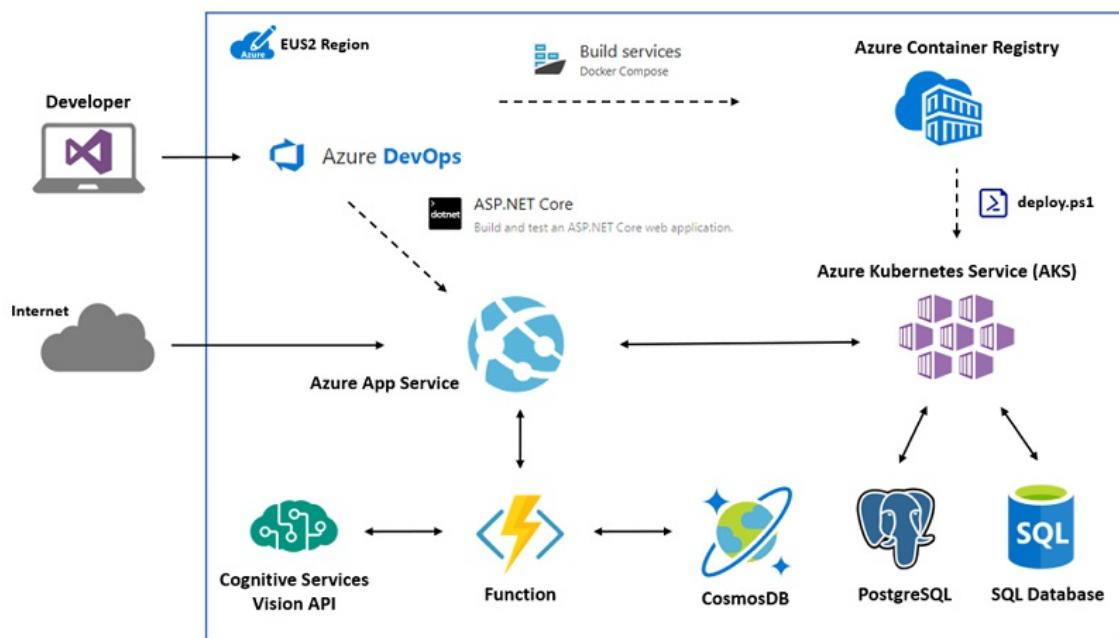


Figure 1: Scenario architecture.

## Solution review

Contoso evaluates the proposed design by putting together a pros and cons list.

CONSIDERATION	DETAILS
Pros	<p>Using PaaS and serverless solutions for the end-to-end deployment significantly reduces the management time that Contoso must provide.</p> <p>Moving to a microservices-based architecture allows Contoso to easily extend the solution over time.</p> <p>New functionality can be brought online without disrupting any of the existing solutions' code bases.</p> <p>The web app will be configured with multiple instances, with no single point of failure.</p> <p>Autoscaling will be enabled so that the application can handle differing traffic volumes.</p> <p>With the move to PaaS services, Contoso can retire out-of-date solutions that run on the Windows Server 2008 R2 operating system.</p> <p>Azure Cosmos DB has built-in fault tolerance, which requires no configuration by Contoso. This means that the data tier is no longer a single point of failover.</p>
Cons	<p>Containers are more complex than other migration options. The learning curve could be an issue for Contoso. They introduce a new level of complexity that provides value in spite of the curve.</p> <p>The operations team at Contoso needs to ramp up to understand and support Azure, containers, and microservices for the application.</p> <p>Contoso hasn't fully implemented DevOps for the entire solution. Contoso needs to consider that for the deployment of services to AKS, Azure Functions, and Azure App Service.</p>

## Migration process

1. Contoso provisions Azure Container Registry, AKS, and Azure Cosmos DB.
2. Contoso provisions the infrastructure for the deployment, including the Azure App Service web app, storage account, function, and API.
3. After the infrastructure is in place, Contoso builds their microservices container images by using Azure DevOps, which pushes the images to the container registry.
4. Contoso deploys these microservices to AKS by using a PowerShell script.
5. Finally, Contoso deploys the function and web app.

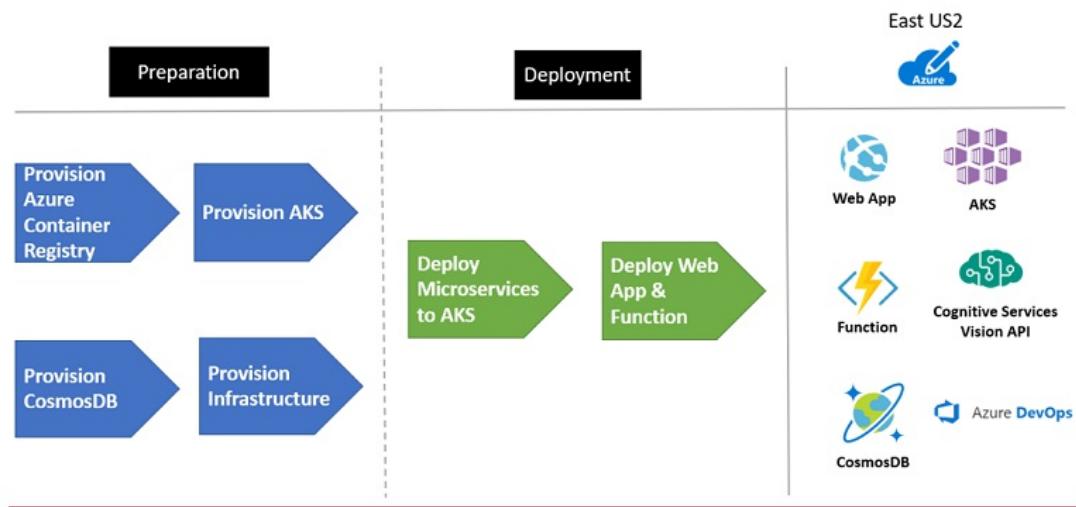


Figure 2: The migration process.

## Azure services

SERVICE	DESCRIPTION	COST
AKS	Simplifies Kubernetes management, deployment, and operations. Provides a fully managed Kubernetes container orchestration service.	AKS is a free service. Pay for only the VMs and the associated storage and networking resources that are consumed. <a href="#">Learn more</a> .
Azure Functions	Accelerates development with an event-driven, serverless compute experience. Scale on demand.	Pay only for consumed resources. Plan is billed based on per-second resource consumption and executions. <a href="#">Learn more</a> .
Azure Container Registry	Stores images for all types of container deployments.	Cost is based on features, storage, and usage duration. <a href="#">Learn more</a> .
Azure App Service	Quickly build, deploy, and scale enterprise-grade web, mobile, and API apps that run on any platform.	App Service plans are billed on a per-second basis. <a href="#">Learn more</a> .

## Prerequisites

Here's what Contoso needs for this scenario:

REQUIREMENTS	DETAILS
Azure subscription	<ul style="list-style-type: none"> <li>Contoso created subscriptions in an earlier article. If you don't have an Azure subscription, create a <a href="#">free account</a>.</li> <li>If you create a free account, you're the admin of your subscription and can perform all actions.</li> <li>If you use an existing subscription and you're not the admin, you need to work with the admin to assign Owner or Contributor permissions to you.</li> </ul>
Azure infrastructure	<ul style="list-style-type: none"> <li>Learn <a href="#">how Contoso set up an Azure infrastructure</a>.</li> </ul>

Requirements	Details
Developer prerequisites	<p>Contoso needs the following tools on a developer workstation:</p> <ul style="list-style-type: none"> <li>• <a href="#">Visual Studio Community 2017 version 15.5</a></li> <li>• .NET workload, enabled</li> <li>• <a href="#">Git</a></li> <li>• <a href="#">Azure PowerShell</a></li> <li>• <a href="#">The Azure CLI</a></li> <li>• <a href="#">Docker Community Edition (Windows 10) or Docker Enterprise Edition (Windows Server)</a>, set to use Windows containers</li> </ul>

## Scenario steps

Here's how Contoso will run the migration:

- **Step 1: Provision AKS and Azure Container Registry.** Contoso provisions the managed AKS cluster and the container registry by using PowerShell.
- **Step 2: Build Docker containers.** Contoso sets up continuous integration (CI) for Docker containers by using Azure DevOps and pushes the containers to the container registry.
- **Step 3: Deploy back-end microservices.** Contoso deploys the rest of the infrastructure that will be used by back-end microservices.
- **Step 4: Deploy front-end infrastructure.** Contoso deploys the front-end infrastructure, including Blob storage for the pet phones, Azure Cosmos DB, and the Computer Vision API.
- **Step 5: Migrate the back end.** Contoso deploys microservices and runs them on AKS to migrate the back end.
- **Step 6: Publish the front end.** Contoso publishes the SmartHotel360 application to Azure App Service along with the function app to be called by the pet service.

## Provision back-end resources

Contoso admins run a deployment script to create the managed Kubernetes cluster by using AKS and Azure Container Registry. The instructions for this section use the [SmartHotel360-Backend](#) GitHub repository. The repository contains all the software for this part of the deployment.

### Ensure that prerequisites are met

Before they start, Contoso admins ensure that all prerequisite software is installed on the dev machine they're using for the deployment. They clone the repository locally to the dev machine by using Git:

```
git clone https://github.com/Microsoft/SmartHotel360-Backend.git
```

### Provision AKS and Azure Container Registry

The Contoso admins provision AKS and Azure Container Registry as follows:

1. In Visual Studio Code, they open the folder and go to the `/deploy/k8s` directory, which contains the script `gen-aks-env.ps1`.
2. They run the script to create the managed Kubernetes cluster, using AKS and Azure Container Registry.

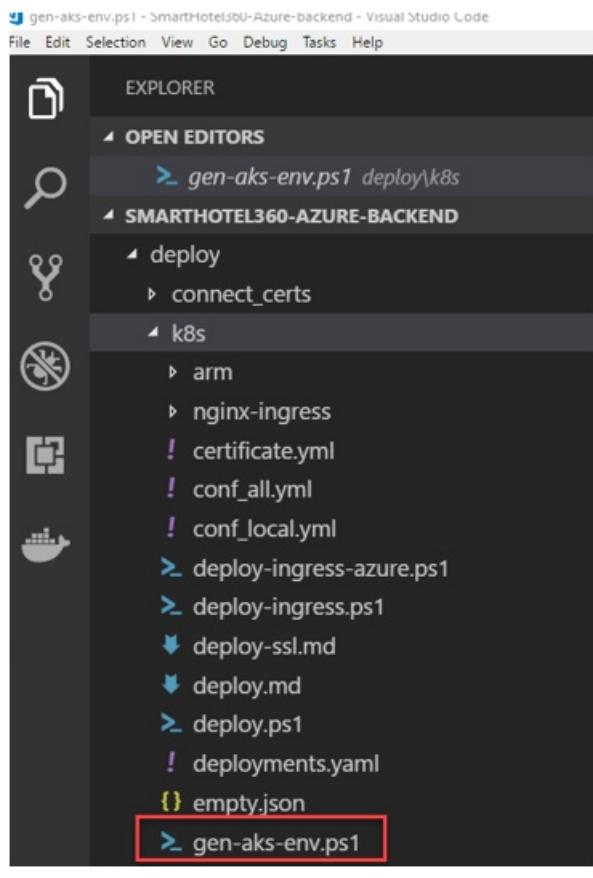


Figure 3: Creating the managed Kubernetes cluster.

- With the file open, they update the \$location parameter to `eastus2`, and save the file.

```
> gen-aks-env.ps1 ×

1  Param(
2      [parameter(Mandatory=$true)][string]$resourceGroupName,
3      [parameter(Mandatory=$false)][string]$location="eastus2", $location="eastus2"
4      [parameter(Mandatory=$false)][string]$registryName,
5      [parameter(Mandatory=$true)][string]$orchestratorName,
6      [parameter(Mandatory=$false)][string]$dnsName="",
7      [parameter(Mandatory=$false)][bool]$createAcr=$true,
8      [parameter(Mandatory=$false)][bool]$createRg=$true,
9      [parameter(Mandatory=$false)][string]$agentVmSize="Standard_D2_v2",
10     [parameter(Mandatory=$false)][Int]$agentCount=1
11 )
```

The screenshot shows the 'gen-aks-env.ps1' file in the Visual Studio Code editor. The code defines a PowerShell parameter block. On line 3, the '\$location' parameter is set to 'eastus2'. This line is highlighted with a red border, indicating it is being edited. The rest of the code defines parameters for resource group name, orchestrator name, registry name, DNS name, and agent configuration.

Figure 4: Saving the file.

- They select **View > Integrated terminal** to open the integrated terminal in Visual Studio Code.

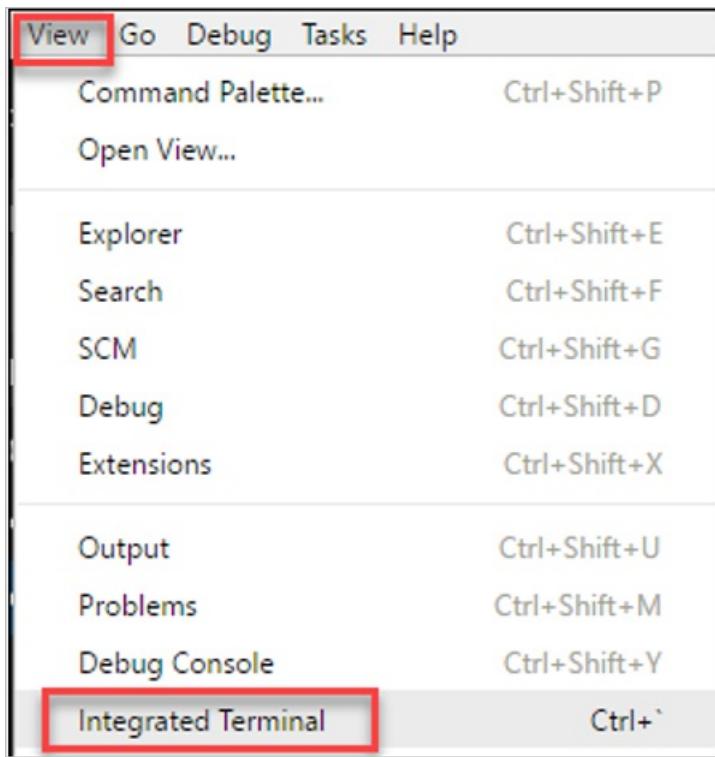


Figure 5: The terminal in Visual Studio Code.

5. In the PowerShell integrated terminal, they sign into Azure using the `Connect-AzureRmAccount` command. For more information, see [Get started with PowerShell](#).

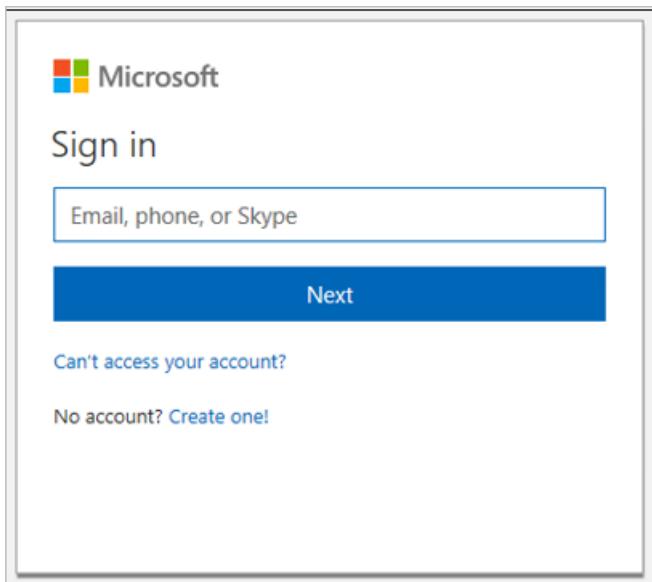


Figure 6: The PowerShell integrated terminal.

6. They authenticate the Azure CLI by running the `az login` command and following the instructions to authenticate using their web browser. Learn more about [logging in with the Azure CLI](#).

# Microsoft Azure Cross-platform Command Line Interface

Click Cancel if this isn't the application you were trying to sign in to on your device.

Continue

Cancel

Figure 7: Authenticating the Azure CLI.

7. They run the following command while passing the resource group name of `ContosoRG`, the name of the AKS cluster `smarhotel1-aks-eus2`, and the new registry name.

```
.\gen-aks-env.ps1 -resourceGroupName ContosoRg -orchestratorName smarhotelakseus2 -registryName smarhotelacreus2
```

NAME	TYPE	LOCATION
smarhotelacreus2	Container registry	East US 2
smarhotelakseus2	Kubernetes service	East US 2

Figure 8: Running the command.

8. Azure creates another resource group that contains the resources for the AKS cluster.

Subscription (change)	Subscription ID	Deployments 1 Succeeded
Tags (change) Click here to add tags		
<input type="text" value="Filter by name..."/> <input type="button" value="All types"/>		
7 items <input type="checkbox"/> Show hidden types	NAME ↑	TYPE ↑
		LOCATION ↑
	aks-agentpool-17518394-nsg	Network security group
	aks-agentpool-17518394-routetable	Route table
	aks-nodepool1-17518394-0	Virtual machine
	aks-nodepool1-17518394-0_OsDisk_1_731e8...	Disk
	aks-nodepool1-17518394-nic-0	Network interface
	aks-vnet-17518394	Virtual network
	nodepool1-availabilitySet-17518394	Availability set

Figure 9: Azure creating a resource group.

- After the deployment is finished, they install the `kubectl` command-line tool. The tool is already installed on the Azure Cloud Shell.

```
az aks install-cli
```

- They verify the connection to the cluster by running the `kubectl get nodes` command. The node has the same name as the VM in the automatically created resource group.

NAME	STATUS	ROLES	AGE	VERSION
aks-nodepool1-17518394-0	Ready	agent	42m	v1.9.6

Figure 10: Verifying the connection to the cluster.

- They run the following command to start the Kubernetes dashboard:

```
az aks browse --resource-group ContosoRG --name smarthotelakseus2
```

- A browser tab opens to the dashboard. This is a tunneled connection that uses the Azure CLI.

The screenshot shows the Kubernetes Dashboard interface. On the left, there's a sidebar with navigation links like Overview, Workloads, Cron Jobs, Daemon Sets, Deployments, Jobs, Pods, Replica Sets, and Replication Controllers. The 'Overview' link is currently selected. The main area has two sections: 'Discovery and Load Balancing' and 'Config and Storage'. Under 'Discovery and Load Balancing', the 'Services' section lists a single service named 'kubernetes'. Its details are shown in a table:

Name	Labels	Cluster IP	Internal endpoints	External endpoints	Age
kubernetes	component: kubernetes, provider: kub	10.0.0.1	kubernetes:443 kubernetes:80	-	50 minutes

Under 'Config and Storage', the 'Secrets' section lists one secret named 'default-token-flh5f' with the following details:

Name	Type	Age
default-token-flh5f	kubernetes.io/service-account-token	50 minutes

Figure 11: A tunneled connection.

## Step 2: Configure the back-end pipeline

### Create an Azure DevOps project and build

Contoso creates an Azure DevOps project, configures a CI build to create the container, and then pushes it to the container registry. The instructions in this section use the [SmartHotel360-Backend](#) repository.

1. From [visualstudio.com](#), they create a new organization ([contosodevops360.visualstudio.com](#)) and configure it to use Git.
2. They create a new project ([SmartHotelBackend](#)), selecting **Git** for version control and **Agile** for the workflow.

## Create new project

X

Project name \*

SmartHotel360Backend

Description

Visibility



Public ⓘ

Anyone on the internet can view the project. Certain features like TFVC are not supported.



Private

Only people you give access to will be able to view this project.

Figure 12: Creating a new project.

3. They import the GitHub repo.

### Import a Git repository

X



Source type

Git

Clone URL \*

`https://github.com/Microsoft/SmartHotel360-Azure-backend.git`

Requires authorization

**Import** **Close**

Figure 13: Importing the GitHub repo.

4. In Pipelines, they select Build and create a new pipeline by using Azure Repos Git as a source from the repository.

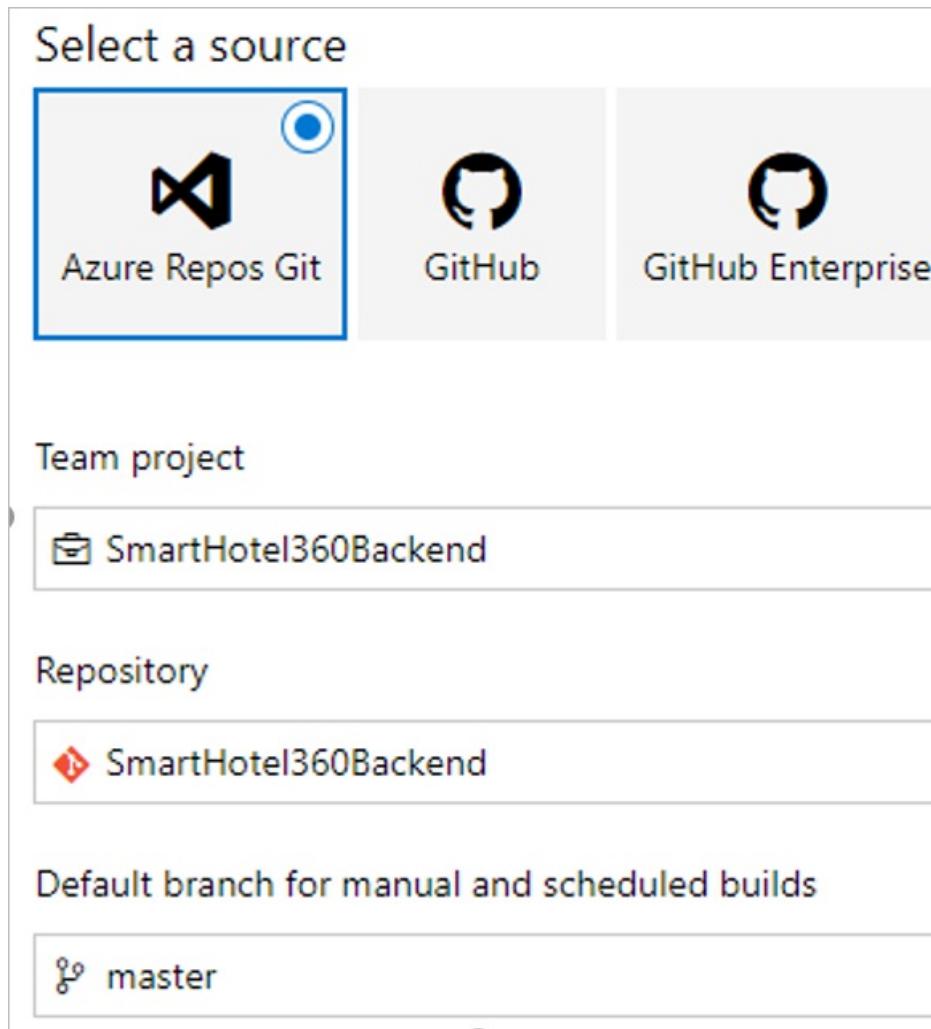


Figure 14: Creating a new pipeline.

5. They select **Empty job**.

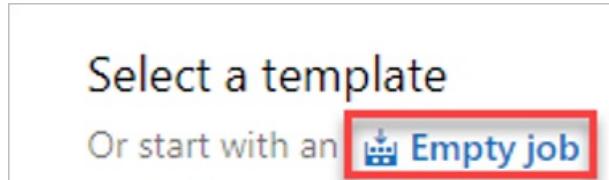


Figure 15: Starting with an empty job.

6. They select **Hosted Linux Preview** for the build pipeline.

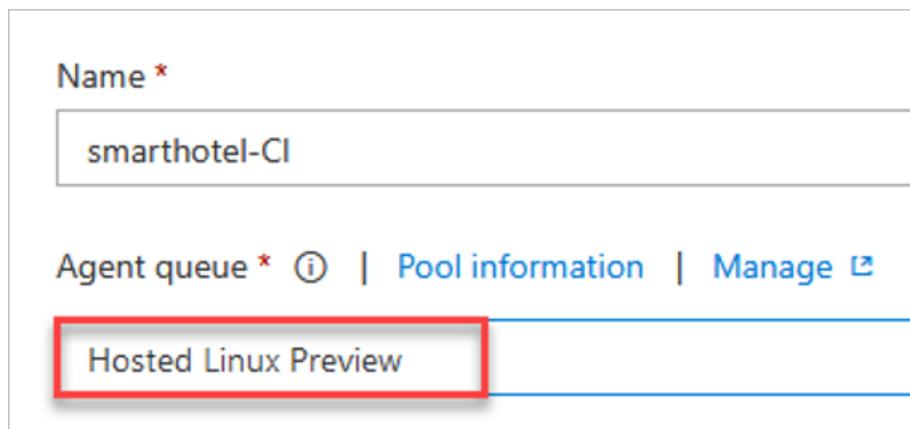


Figure 16: Setting up the build pipeline.

7. In Phase 1, they add a Docker Compose task. This task builds the Docker Compose.

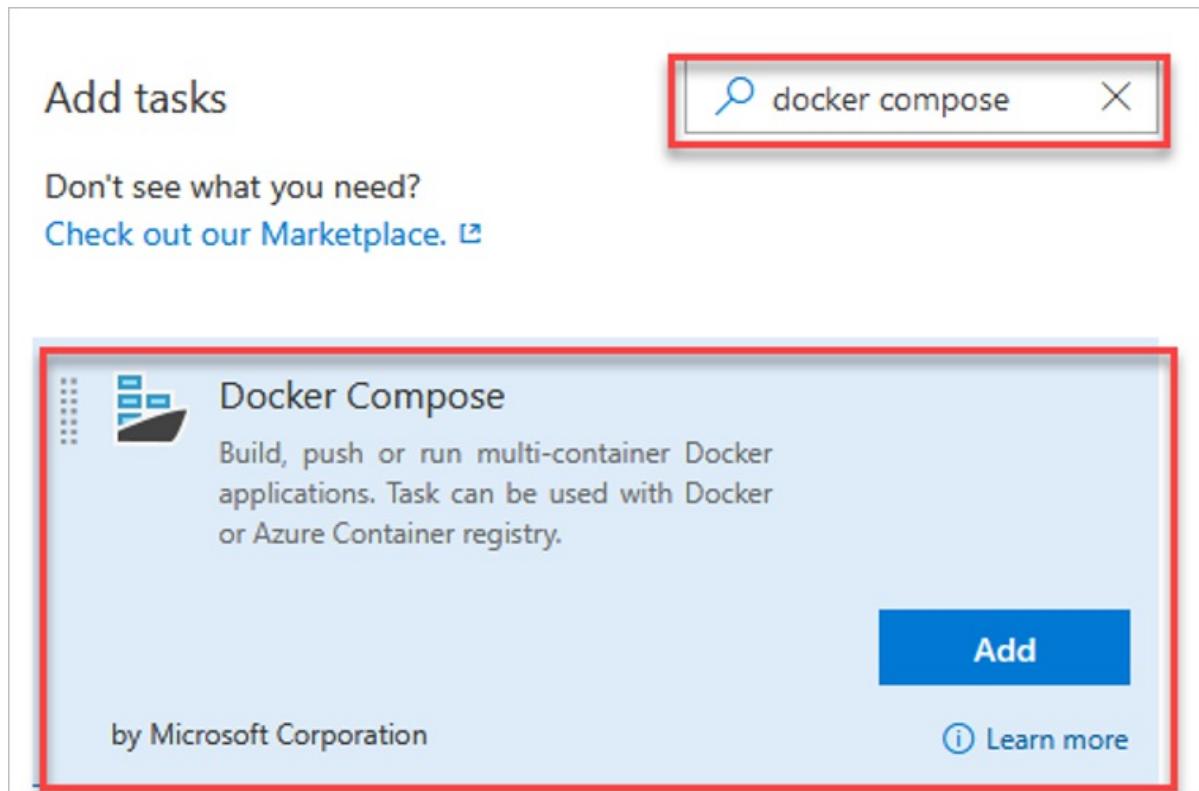


Figure 17: Building the Docker Compose.

8. They repeat and add another **Docker Compose** task. This one pushes the containers to the container registry.

smarthotel-Cl

Tasks Variables Triggers Options Retention

Process

Build process

Get sources

smarthotel master

Phase 1

Run on agent

Run a Docker Compose command

Some settings need attention

Run a Docker Compose command

Some settings need attention

Figure 18: Adding another Docker Compose task.

9. They select the first task to build and configure the build with the Azure subscription, authorization, and

Container Registry.

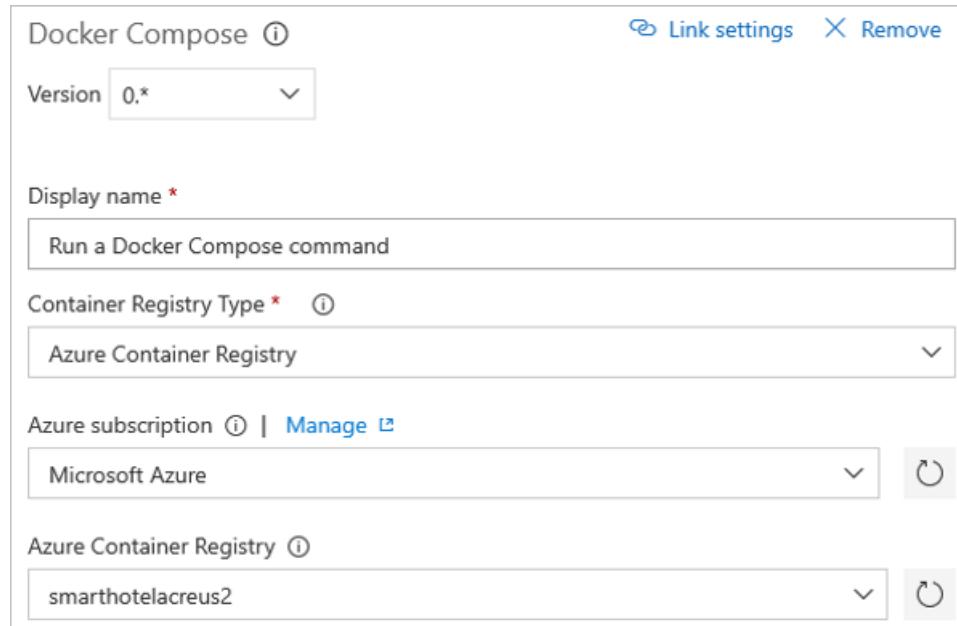


Figure 19: Building and configuring the build.

10. They specify the path of the `docker-compose.yaml` file in the `src` folder of the repo. They choose to build service images and include the latest tag. When the action changes to **Build service images**, the name of the Azure DevOps task changes to **Build services automatically**.

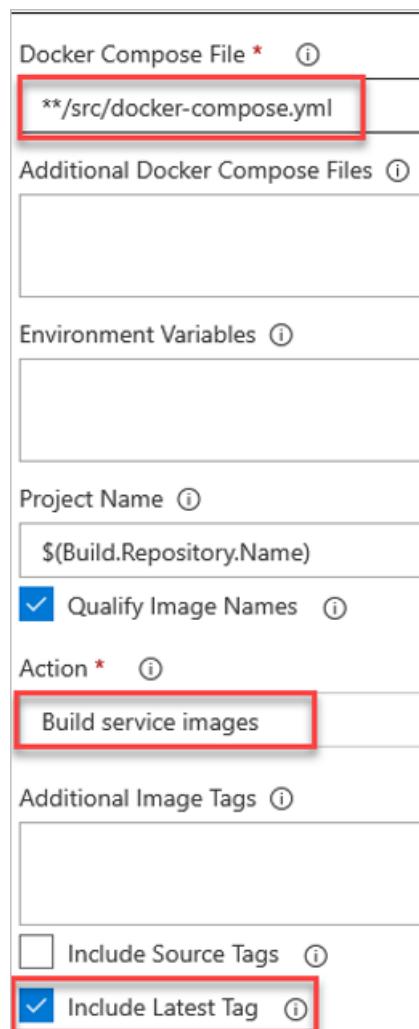


Figure 20: The specifics of the task.

11. Now, they configure the second Docker task (to push). They select the subscription and the container

registry ( smarthotelacreus2 ).

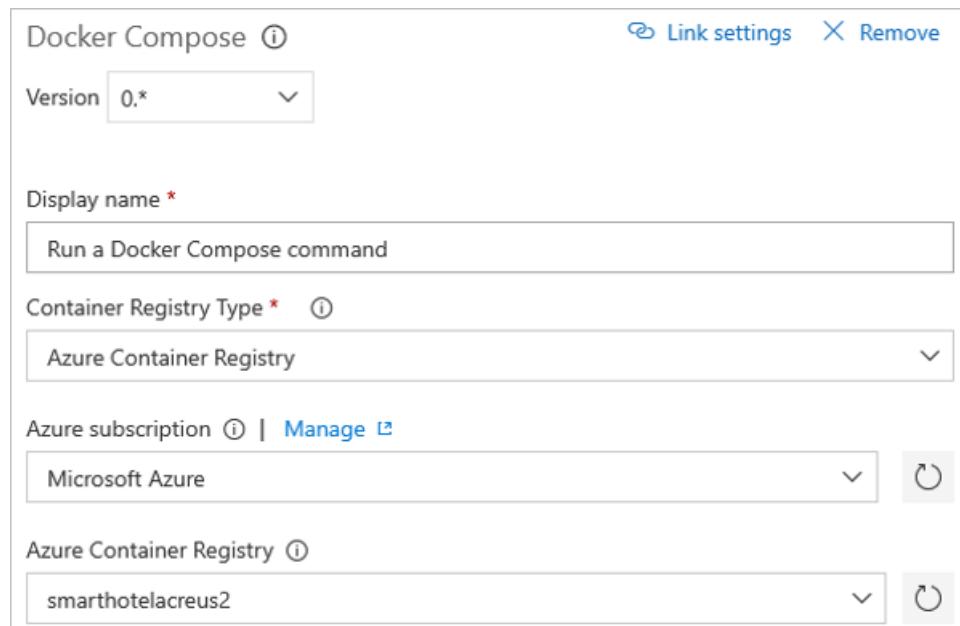


Figure 21: Configuring the second Docker task.

12. They enter the `docker-compose.yaml` file name and select **Push service images**, including the latest tag. When the action changes to **Push service images**, the name of the Azure DevOps task changes to **Push services automatically**.

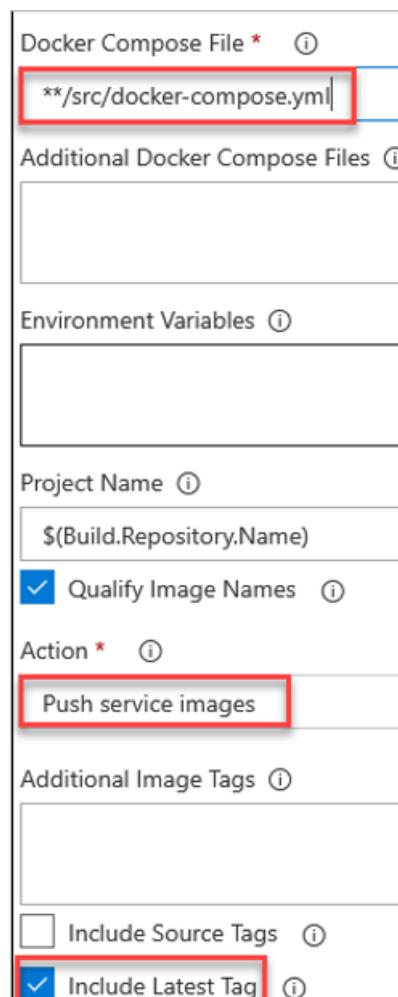


Figure 22: Changing the Azure DevOps task name.

13. With the Azure DevOps tasks configured, Contoso saves the build pipeline and starts the build process.

The screenshot shows the Azure DevOps CI pipeline editor interface. At the top, there are tabs for Tasks, Variables, Triggers, Options, Retention, and History. To the right of these is a 'Save & queue' button, which is highlighted with a red box. Below the tabs, there's a 'Process' section with a 'Build process' step. Underneath is a 'Get sources' step for the 'smarthotel' repository, specifically the 'master' branch. The main area contains a 'Phase 1' section with a 'Run on agent' step. This phase includes two tasks: 'Build services' (using Docker Compose) and 'Push services' (also using Docker Compose). The 'Push services' task has a checkmark icon and a three-dot ellipsis icon.

Figure 23: Starting the build process.

14. They select the build job to check progress.

<p>► Build 9</p> <p>► Phase 1</p> <ul style="list-style-type: none"> <li>► Job</li> <li>✓ Initialize Agent</li> <li>✓ Initialize Job</li> <li>✓ Get Sources</li> <li>► Build services</li> <li>▫ Push services</li> <li>▫ Post Job Cleanup</li> </ul>	<p>smarthotel-CI / Build 9 / Phase 1 / Job</p> <p><a href="#">Edit build definition</a> <a href="#">Cancel</a> <a href="#">Queue new build...</a> <a href="#">Download all logs as zip</a></p> <p><b>Build Started</b></p> <p>Job  Running for 23 seconds (Hosted Agent)</p> <p>Console Timeline Code coverage* Tests</p> <pre>/usr/local/bin/docker-compose -f /opt/vsts/work/1/s/src/docker-compose.yml -f /o sql-data uses an image, skipping Building configuration-api Step 1/13 : FROM microsoft/aspnetcore:2.0.3 AS base 2.0.3: Pulling from microsoft/aspnetcore Digest: sha256:15ba4ece71c4219b2485851dc09dc80fb463ea68d053bd78e78553ea40385e48 Status: Downloaded newer image for microsoft/aspnetcore:2.0.3 --&gt; 7f83f41eee6d Step 2/13 : WORKDIR /app Removing intermediate container b5685681cedb --&gt; e76abe672504 Step 3/13 : EXPOSE 80 --&gt; Running in f53bdedc9019 Removing intermediate container f53bdedc9019 --&gt; 02b9f0690b1a Step 4/13 : FROM microsoft/aspnetcore-build:2.0.3 AS build 2.0.3: Pulling from microsoft/aspnetcore-build</pre>
<p>✓ Build 9</p> <p>✓ Phase 1</p> <ul style="list-style-type: none"> <li>✓ Job</li> <li>✓ Initialize Agent</li> <li>✓ Initialize Job</li> <li>✓ Get Sources</li> <li>✓ Build services</li> <li>✓ Push services</li> <li>✓ Post Job Cleanup</li> <li>✓ Report build status</li> </ul>	<p>smarthotel-CI / Build 9 / Phase 1 / Job</p> <p><a href="#">Edit build definition</a> <a href="#">Queue new build...</a> <a href="#">Do</a></p> <p><b>Build succeeded</b></p> <p>Job  Ran for 9.2 minutes (Hosted Agent),</p> <p>Console Logs Timeline Code coverage* Tests</p> <pre>20f08d1ba4f1: Preparing a130cc33ffce: Preparing 3fa6e458af6f: Preparing 0f3a12fef684: Preparing 979fc76b7e77: Waiting 20f08d1ba4f1: Waiting</pre>

Figure 24: Checking the progress.

15. After the build finishes, the container registry shows the new repos, which are populated with the containers used by the microservices.

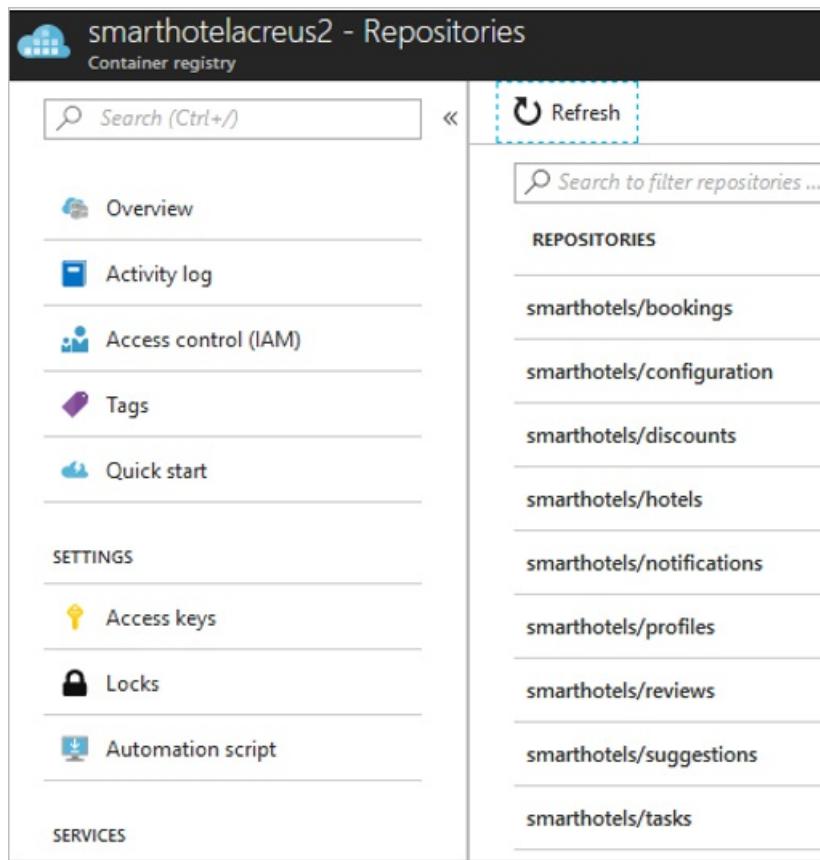


Figure 25: Viewing new repos after the build finishes.

## Deploy the back-end infrastructure

With the AKS cluster created and the Docker images built, Contoso admins now deploy the rest of the infrastructure that will be used by back-end microservices.

- Instructions in this section use the [SmartHotel360-Backend](#) repo.
- In the `/deploy/k8s/arm` folder, there's a single script to create all items.

The admins deploy the infrastructure as follows:

1. They open a developer command prompt and then use the command `az login` for the Azure subscription.
2. They use the `deploy.cmd` file to deploy the Azure resources in the `ContosoRG` resource group and `East US 2` region by typing the following command:

```
.\deploy.cmd azuredeploy ContosoRG -c eastus2
```

NAME ↑↓	TYPE ↑↓
 appinsightspublicql6hxie4iqrwq	Application Insights
 sh360postgrespublicql6hxie4iqrwq	Azure Database for PostgreSQL server
 sh360publicql6hxie4iqrwq	Storage account
 sh360sqlpublicql6hxie4iqrwq	SQL server
 BookingsDb (sh360sqlpublicql6hxie4iqrwq/BookingsDb)	SQL database
 HotelsDb (sh360sqlpublicql6hxie4iqrwq/HotelsDb)	SQL database
 ProfilesDb (sh360sqlpublicql6hxie4iqrwq/ProfilesDb)	SQL database
 SuggestionsDb (sh360sqlpublicql6hxie4iqrwq/Suggestions...)	SQL database
 TasksDb (sh360sqlpublicql6hxie4iqrwq/TasksDb)	SQL database
 smarhotelacreus2	Container registry
 smarhotelakseus2	Kubernetes service

Figure 26: Deploying the back end.

- In the Azure portal, they capture the connection string for each database for later use.

```
File Edit Format View Help
DataConnectStrings.txt - Notepad
Database connection strings
-----
PostgreSQL
jdbc:postgresql://sh360postgrespublicql6hxie4iqrwq.postgres.database.windows.net:5432/BooksingsDB?sslmode=require&user=sa&password=Passw0rd&encrypt=true&port=5432

BooksingsDB
Server=tcp:sh360sqlpublicql6hxie4iqrwq.database.windows.net,1433;

HotelsDB
Server=tcp:sh360sqlpublicql6hxie4iqrwq.database.windows.net,1433;

ProfilesDB
Server=tcp:sh360sqlpublicql6hxie4iqrwq.database.windows.net,1433;

SuggestionsDB
Server=tcp:sh360sqlpublicql6hxie4iqrwq.database.windows.net,1433;

TasksDB
Server=tcp:sh360sqlpublicql6hxie4iqrwq.database.windows.net,1433;
```

Figure 27: Capturing the connection string for each database.

## Create the back-end release pipeline

Now, Contoso admins do the following:

- Deploy the NGINX ingress controller to allow inbound traffic to the services.
- Deploy the microservices to the AKS cluster.
- As a first step, admins update the connection strings to the microservices by using Azure DevOps. They then configure a new Azure DevOps release pipeline to deploy the microservices.
- The instructions in this section use the [SmartHotel360-Backend](#) repo.
- Some of the configuration settings (for example, Active Directory B2C) aren't covered in this article. For more information about these settings, review the previously mentioned SmartHotel360-Backend repo.

The admins create the pipeline:

- In Visual Studio, they update the `/deploy/k8s/config_local.yml` file with the database connection information that they noted earlier.

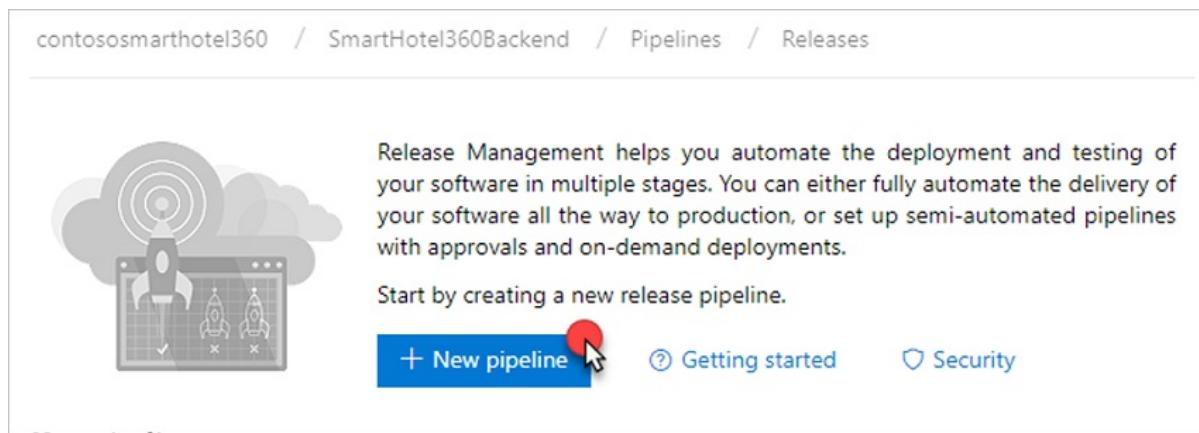


Figure 28: Database connections.

2. They open Azure DevOps and, in the SmartHotel360 project, they select + New pipeline on the Releases pane.

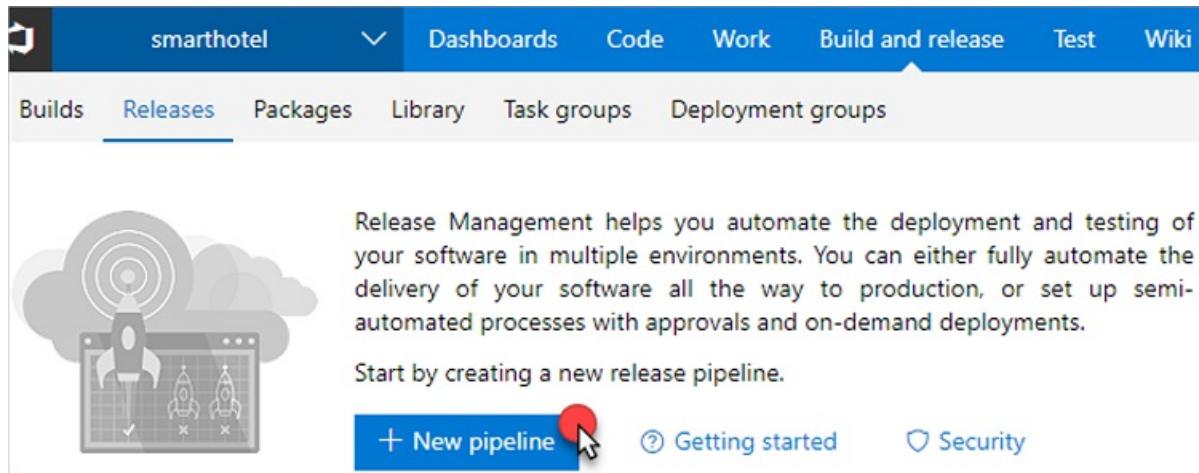
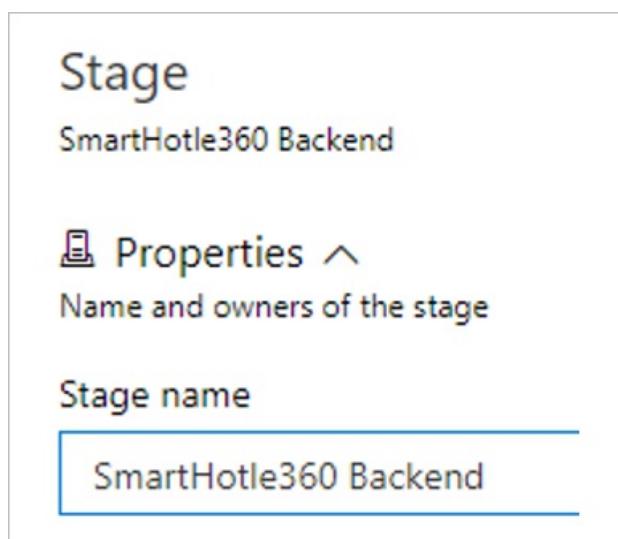


Figure 29: Creating a new pipeline.

3. They select Empty Job to start the pipeline without a template.
4. They provide the stage and pipeline names.



\_Figure 30: The stage name.\_

All pipelines >  SmartHotel 360 Backend

Figure 31: The pipeline name.

5. They add an artifact.

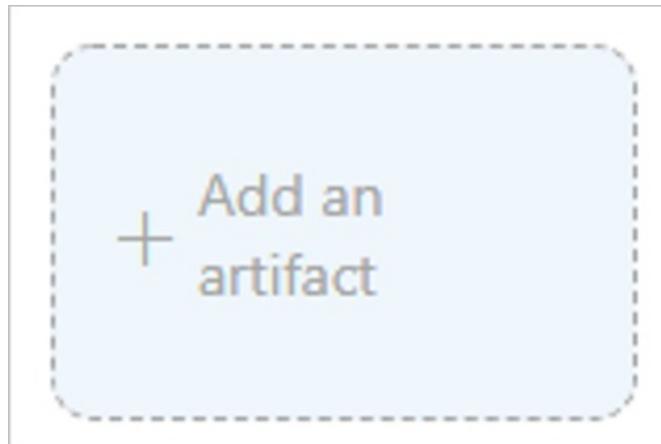


Figure 32: Adding an artifact.

6. They select Git as the source type and specify the project, source, and master branch for the SmartHotel360 application.

Add an artifact

Source type

 Build     Git     GitHub     Team Found...

[4 more artifact types ▾](#)

Project \* i

SmartHotelBackend

Source (repository) \* i

SmartHotelBackend

Default branch \* i

master

This is a screenshot of the "Add an artifact" configuration page. At the top, it says "Add an artifact". Below that, under "Source type", there are four options: "Build" (with a build icon), "Git" (with a git icon), "GitHub" (with a GitHub icon), and "Team Foundation..." (with a TFS icon). The "Git" option is selected, indicated by a blue border around its icon and the word "Git" below it. A red circle with a white arrow points to the "Git" icon. Below the source type, there are three dropdown menus: "Project" set to "SmartHotelBackend", "Source (repository)" set to "SmartHotelBackend", and "Default branch" set to "master". Each dropdown has a small "i" icon next to it, likely indicating an informational tooltip.

Figure 33: The artifact settings pane.

7. They select the task link.

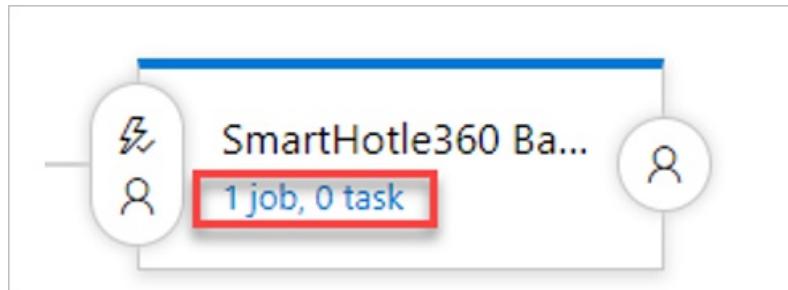


Figure 34: The task link.

8. They add a new Azure PowerShell task so that they can run a PowerShell script in an Azure environment.

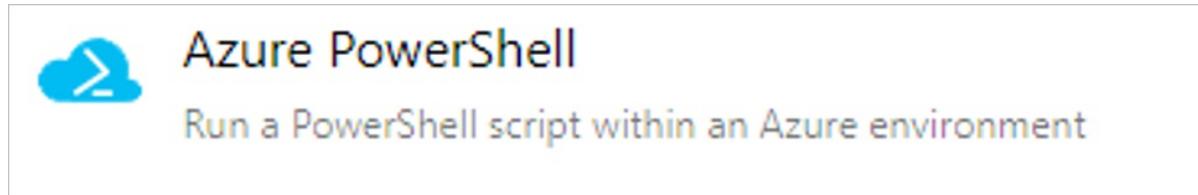


Figure 35: Adding a new PowerShell task.

9. They select the Azure subscription for the task and select the `deploy.ps1` script from the Git repo.

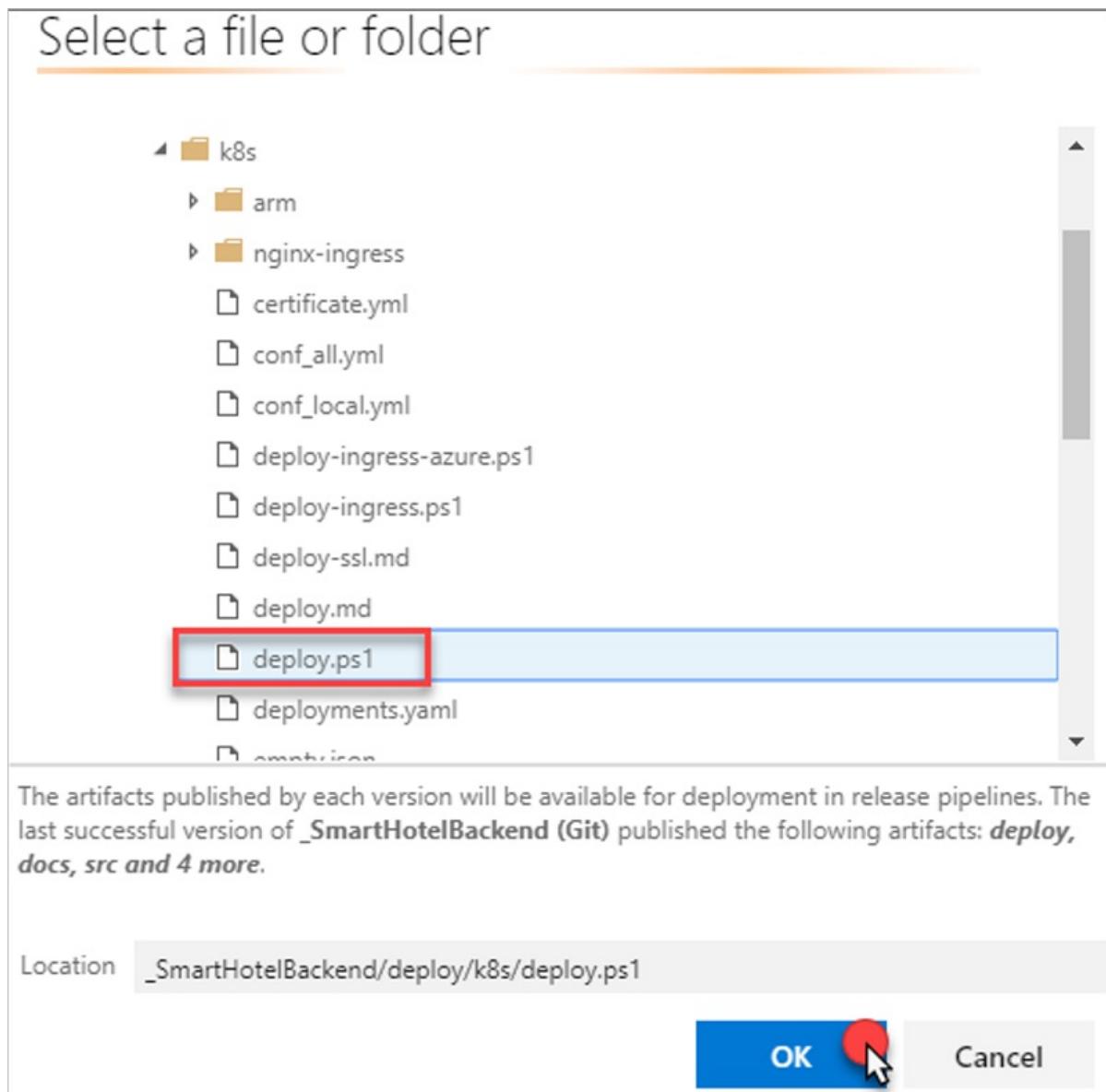


Figure 36: Running the script.

10. They add arguments to the script. The script will delete all cluster content (except ingress and ingress controller), and deploy the microservices.

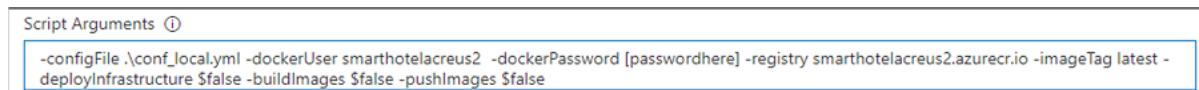


Figure 37: Adding arguments to the script.

11. They set the preferred Azure PowerShell version to the latest version, and save the pipeline.
12. They go back to the Create a new release pane and manually create a new release.

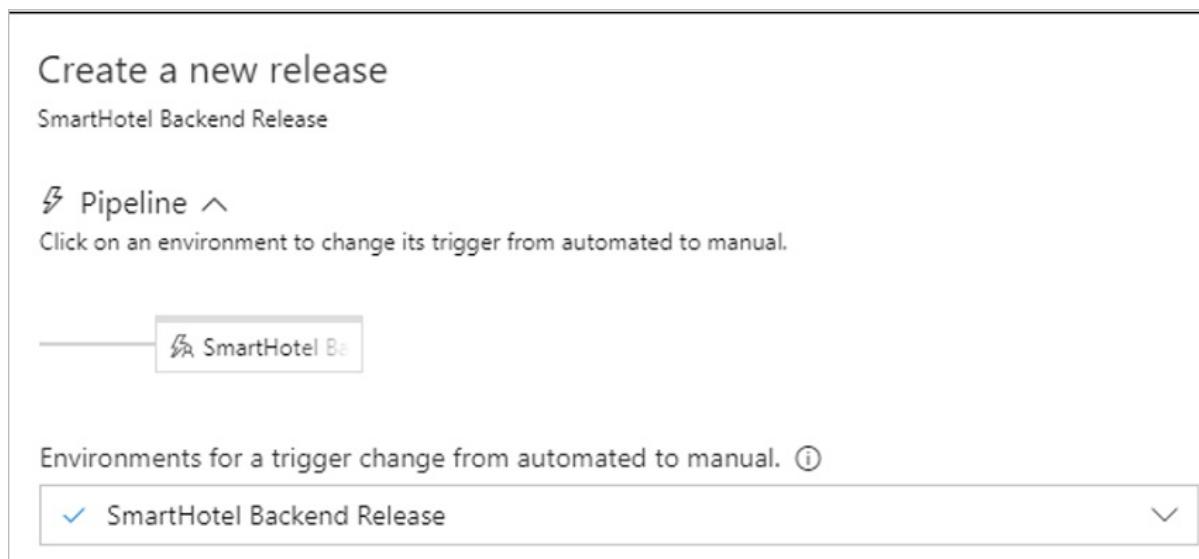


Figure 38: Manually creating a new release.

13. After they create the release, they select it and, under **Actions**, they select **Deploy**.

SmartHotel Backend Release / Release-1

Summary Environments Artifacts Variables General Commits

⟳ | ⚡ Deploy ▾ Save Abandon ↗ Release (pipeline)

Details

No description 🖊

⚡ smarthotel / 872aa5b7 (Git) ⚡ master

Environments

Environment	Actions	Deployment status	Triggered
SmartHotel Backend...	...	NOT DEPLOYED ⓘ	

Issues

No issues reported in thi

Figure 39: Deploying a release.

14. When the deployment is complete, they run the following command to check the status of services, using

the Azure Cloud Shell: `kubectl get services`.

## Step 3: Provision front-end services

Contoso admins need to deploy the infrastructure that will be used by the front-end applications. They create:

- A Blob storage container to store the pet images.
- An Azure Cosmos DB database to store documents containing pet information.
- The Computer Vision API for the website.

Instructions for this section use the [SmartHotel360-website](#) repo.

### Create Blob storage containers

1. In the Azure portal, the admins open the storage account that was created, and then select **Blobs**.
2. They create a new container named `Pets` with the public-access level set for the container. Users will upload their pet photos to this container.

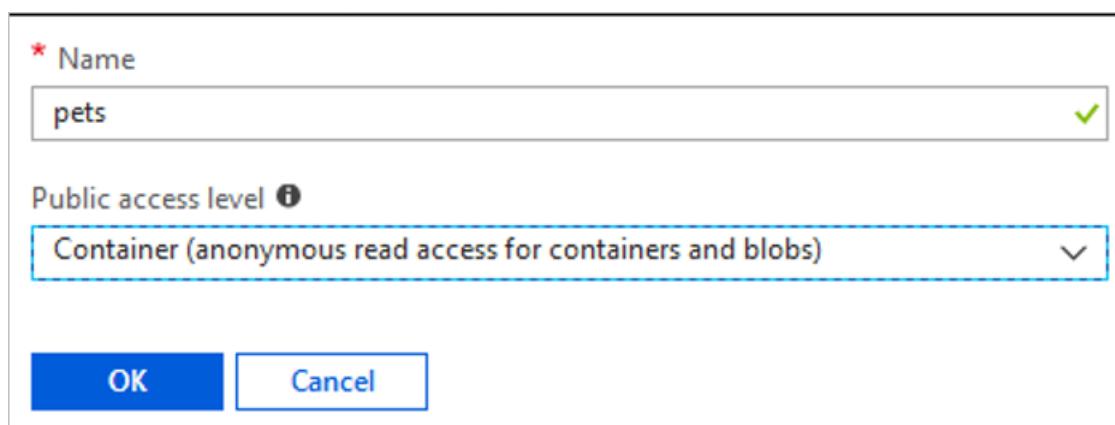


Figure 40: Creating a new container.

3. They create a second new container named `settings`. A file with all the front-end app settings will be placed in this container.

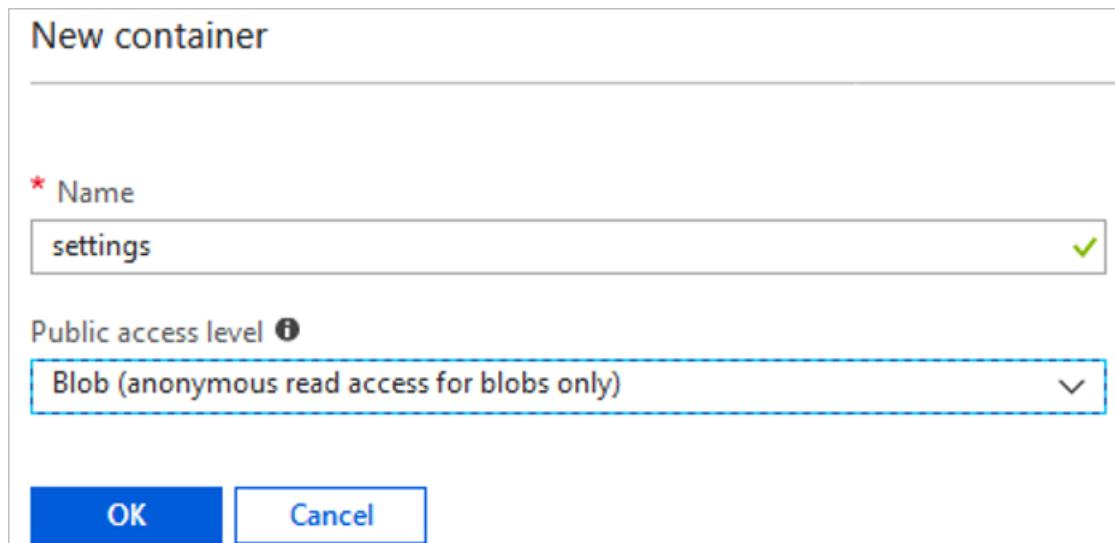


Figure 41: Creating a second container.

4. They capture the access details for the storage account in a text file for future reference.

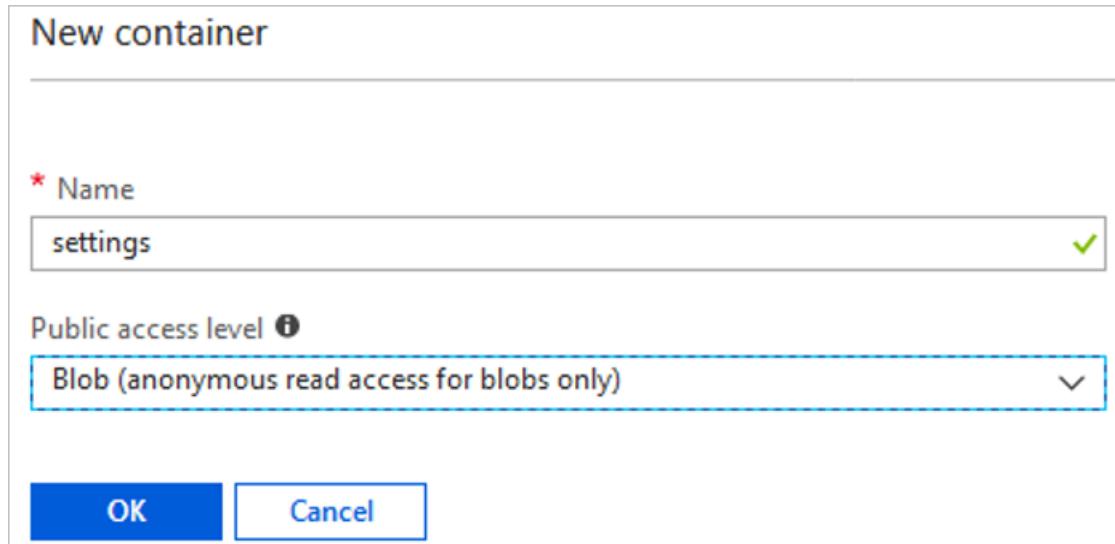


Figure 42: A text file capturing access details.

### Provision an Azure Cosmos DB database

Contoso admins provision an Azure Cosmos DB database to be used for pet information.

1. They create an Azure Cosmos DB database in Azure Marketplace.

Azure Marketplace	See all	Featured	See all
Get started		SQL Database <a href="#">Quickstart tutorial</a>	
Recently created			
Compute		SQL Data Warehouse <a href="#">Quickstart tutorial</a>	
Networking			
Storage		SQL Elastic database pool <a href="#">Learn more</a>	
Web			
Mobile			
Containers			
Databases		Azure Database for MySQL <a href="#">Quickstart tutorial</a>	
Analytics		Azure Database for PostgreSQL <a href="#">Quickstart tutorial</a>	
AI + Machine Learning			
Internet of Things		SQL Server 2017 Enterprise Windows Server 2016 <a href="#">Learn more</a>	
Integration			
Security			
Identity		Azure Cosmos DB <a href="#">Quickstart tutorial</a>	

Figure 43: Creating an Azure Cosmos DB database.

2. They specify a name `contososmarthotel1`, select the SQL API, and place it in the production resource group `ContosoRG` in the main region `East US 2`.

Azure Cosmos DB

New account

\* ID  
contosomarhotel ✓  
documents.azure.com

\* API ⓘ  
SQL

\* Subscription  
▼

\* Resource Group  
 Create new  Use existing  
ContosoRG

\* Location  
East US 2

Enable geo-redundancy ⓘ

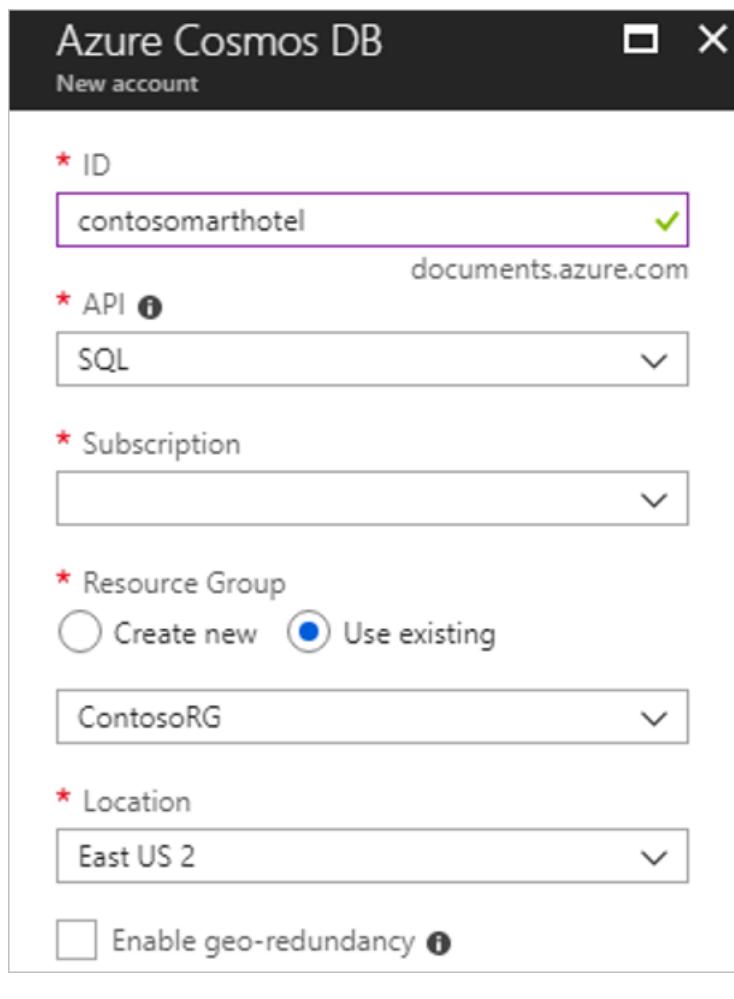


Figure 44: Naming an Azure Cosmos DB database.

3. They add a new collection to the database, with default capacity and throughput.

Add Collection

\* Database id ⓘ  
 Create new  Use existing  
pets

Provision database throughput ⓘ

\* Collection Id ⓘ  
checks

\* Storage capacity ⓘ  
 Fixed (10 GB)  Unlimited

\* Throughput (400 - 10,000 RU/s) ⓘ  
5000 □ - +

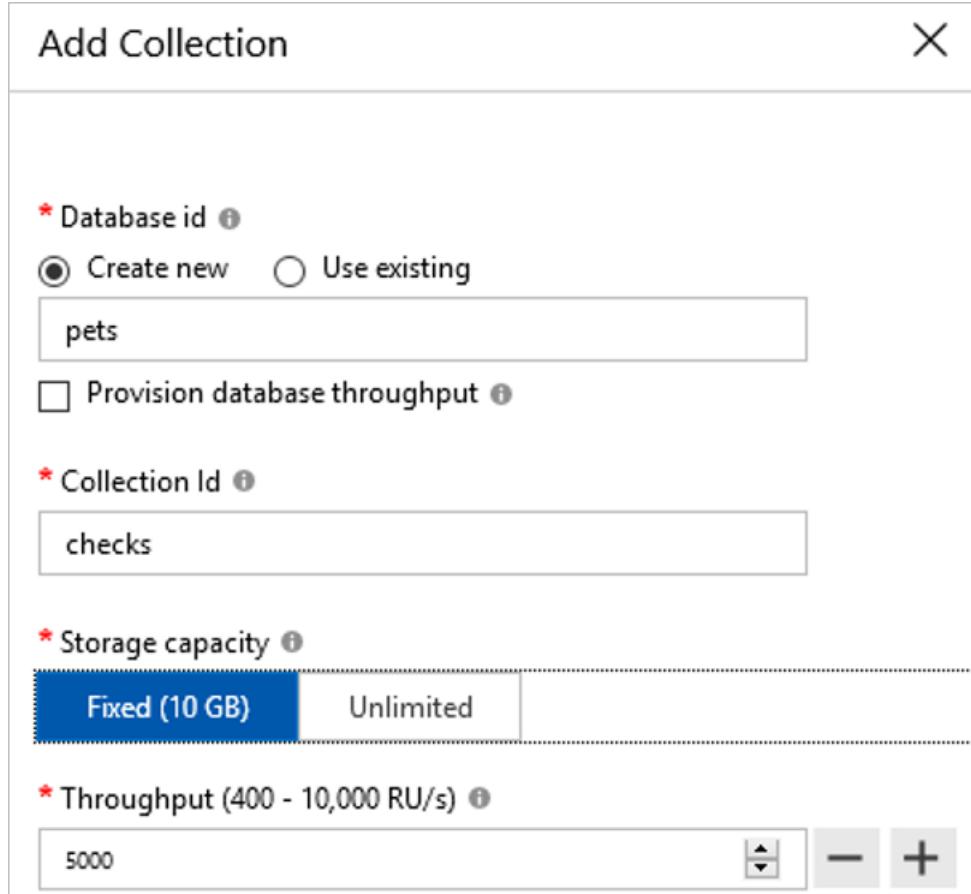
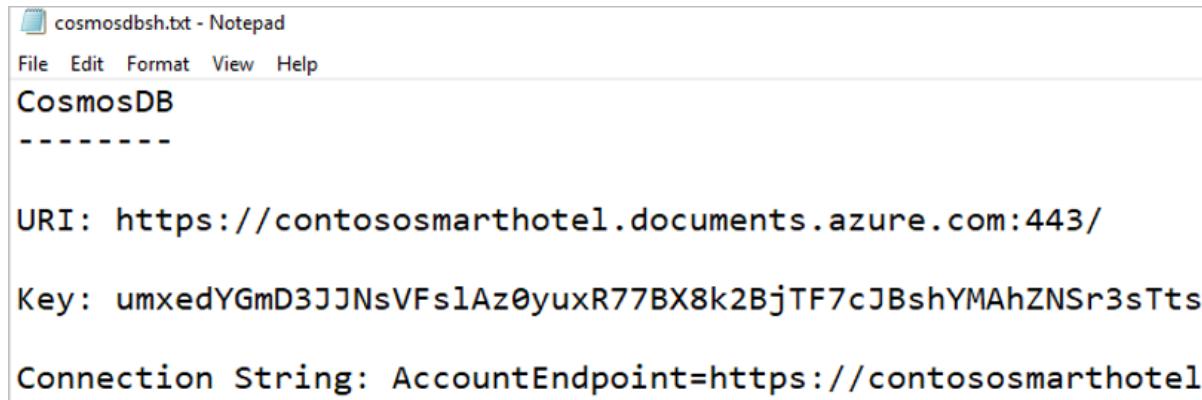


Figure 45: Adding a new collection to the database.

4. They note the connection information for the database for future reference.



The screenshot shows a Notepad window with the following content:

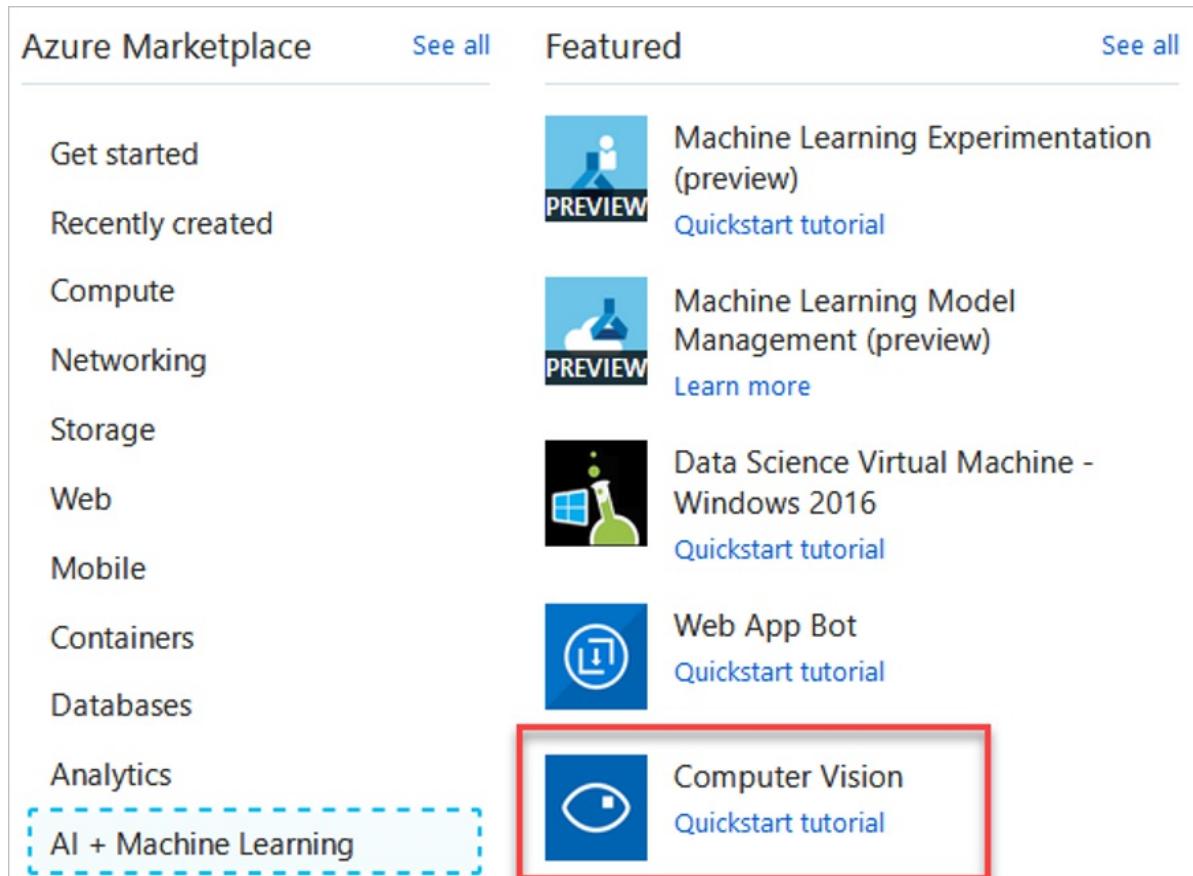
```
cosmosdbsh.txt - Notepad
File Edit Format View Help
CosmosDB
-----
URI: https://contososmarthotel.documents.azure.com:443/
Key: umxedYGmD3JJNsVFslAz0yuxR77BX8k2BjTF7cJBshYMAhZNSr3sTts
Connection String: AccountEndpoint=https://contososmarthotel
```

Figure 46: The connection information for the database.

### Provision the Computer Vision API

Contoso admins provision the Computer Vision API. The API will be called by the function, to evaluate pictures that are uploaded by users.

1. The admins create a Computer Vision instance in Azure Marketplace.



The screenshot shows the Azure Marketplace interface. On the left, there's a sidebar with categories like Get started, Recently created, Compute, Networking, Storage, Web, Mobile, Containers, Databases, Analytics, and AI + Machine Learning. The AI + Machine Learning category is highlighted with a blue dashed box. On the right, under the 'Featured' section, there are several items:

- Machine Learning Experimentation (preview) - PREVIEW icon, Quickstart tutorial link.
- Machine Learning Model Management (preview) - PREVIEW icon, Learn more link.
- Data Science Virtual Machine - Windows 2016 - icon, Quickstart tutorial link.
- Web App Bot - icon, Quickstart tutorial link.
- Computer Vision - icon, Quickstart tutorial link. This item is highlighted with a red box.

Figure 47: A new instance in Azure Marketplace.

2. They provision the API (`smarthotelpets`) in the production resource group `ContosoRG`, in the main region (`East US 2`).

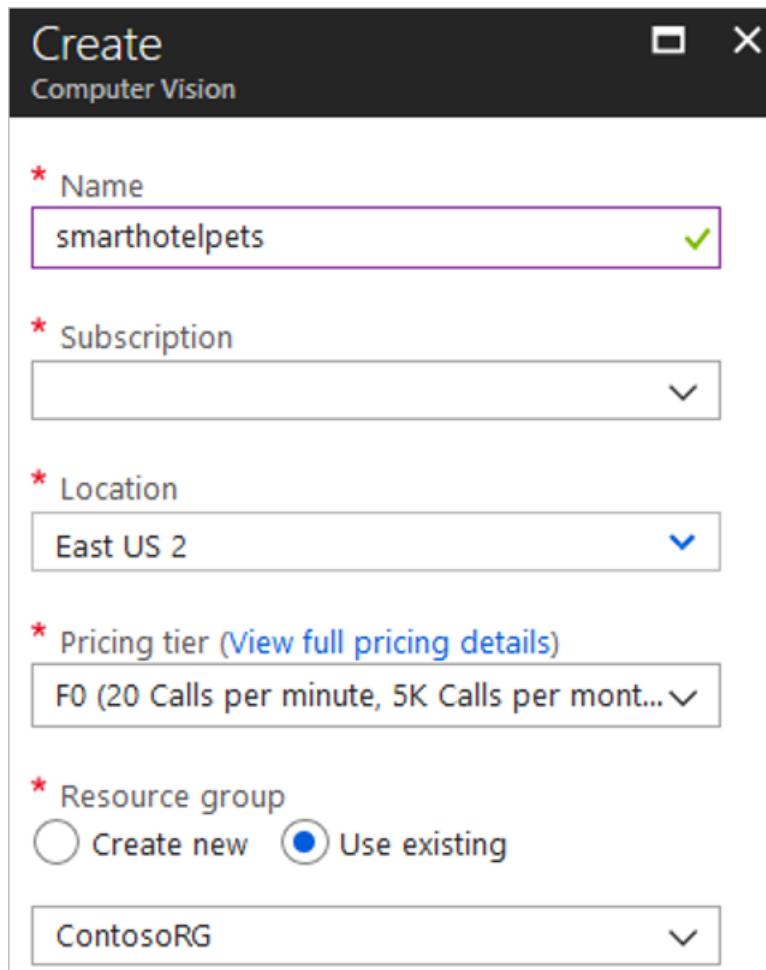


Figure 48: Provisioning an API in a production resource group.

3. They save the connection settings for the API to a text file for later reference.

```
visionapi.txt - Notepad
File Edit Format View Help
Computer Vision API
-----
Name:
smarthotelpets
Key:
[REDACTED]
Endpoint:
https://eastus2.api.cognitive.microsoft.com/vision/v1.0
```

Figure 49: Saving an API's connection settings.

### Provision the Azure web app

Contoso admins provision the web app by using the Azure portal.

1. They select **Web App** in the portal.

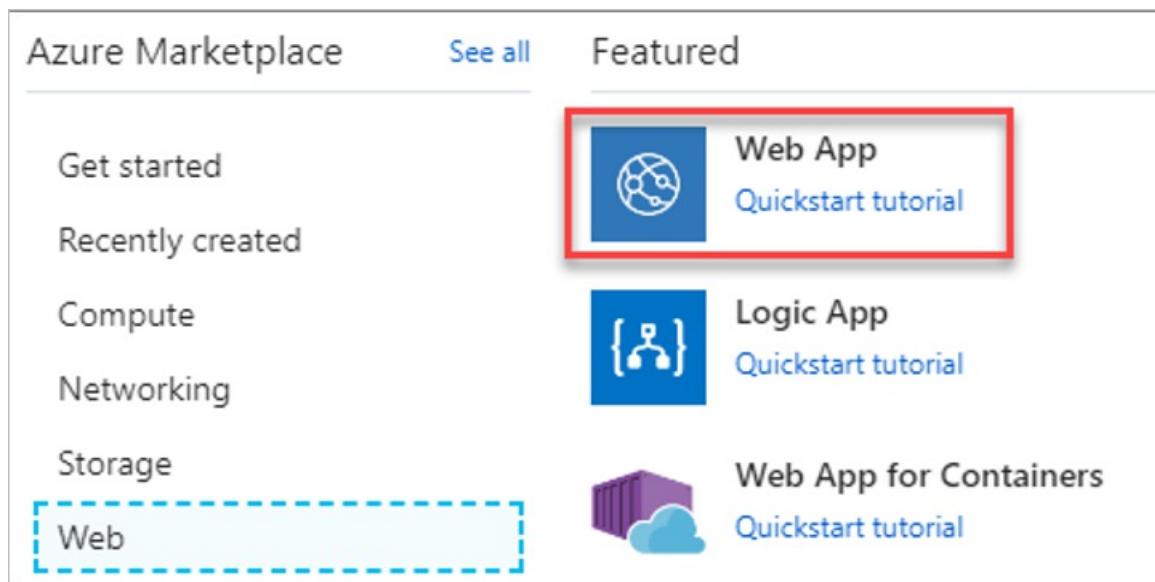


Figure 50: Selecting the web app.

2. They provide a web app name (`smarthotelcontoso`), run it on Windows, and place it in the production resource group `ContosoRG`. They create a new Application Insights instance for application monitoring.

**Web App**

Create

\* App name  
smarthotelcontoso

.azurewebsites.net

\* Subscription

\* Resource Group   
 Create new  Use existing

ContosoRG

\* OS Windows Linux Docker

---

\* App Service plan/Location >  
SH-APP-PLAN(East US 2)

---

Application Insights On Off

---

\* Application Insights Location   
East US

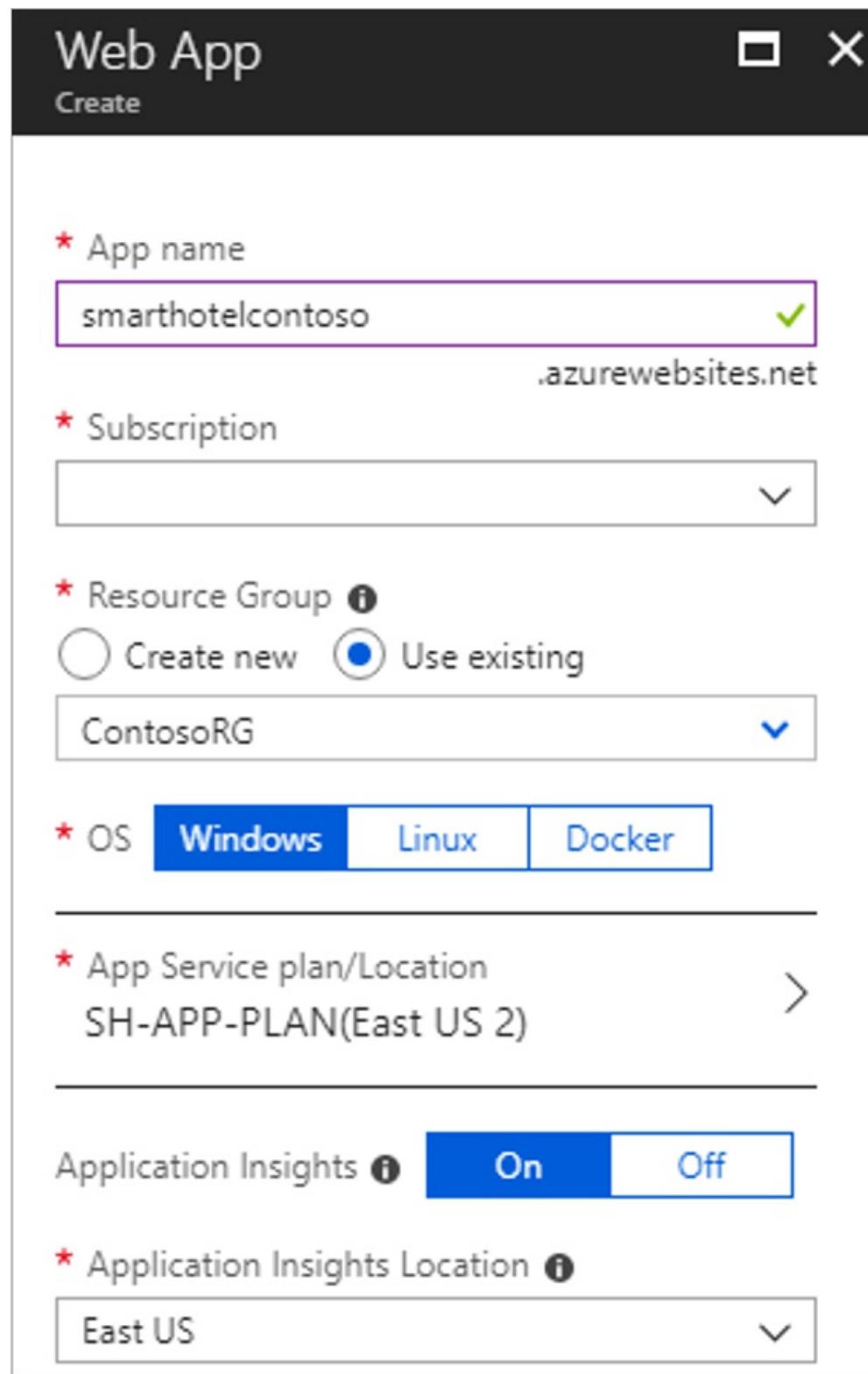


Figure 51: The web app name.

3. After they're done, the admins browse to the address of the application to check on whether it has been created successfully.
4. In the Azure portal, they create a staging slot for the code. The pipeline will be deployed to this slot. This approach ensures that code isn't put into production until the admins perform a release.

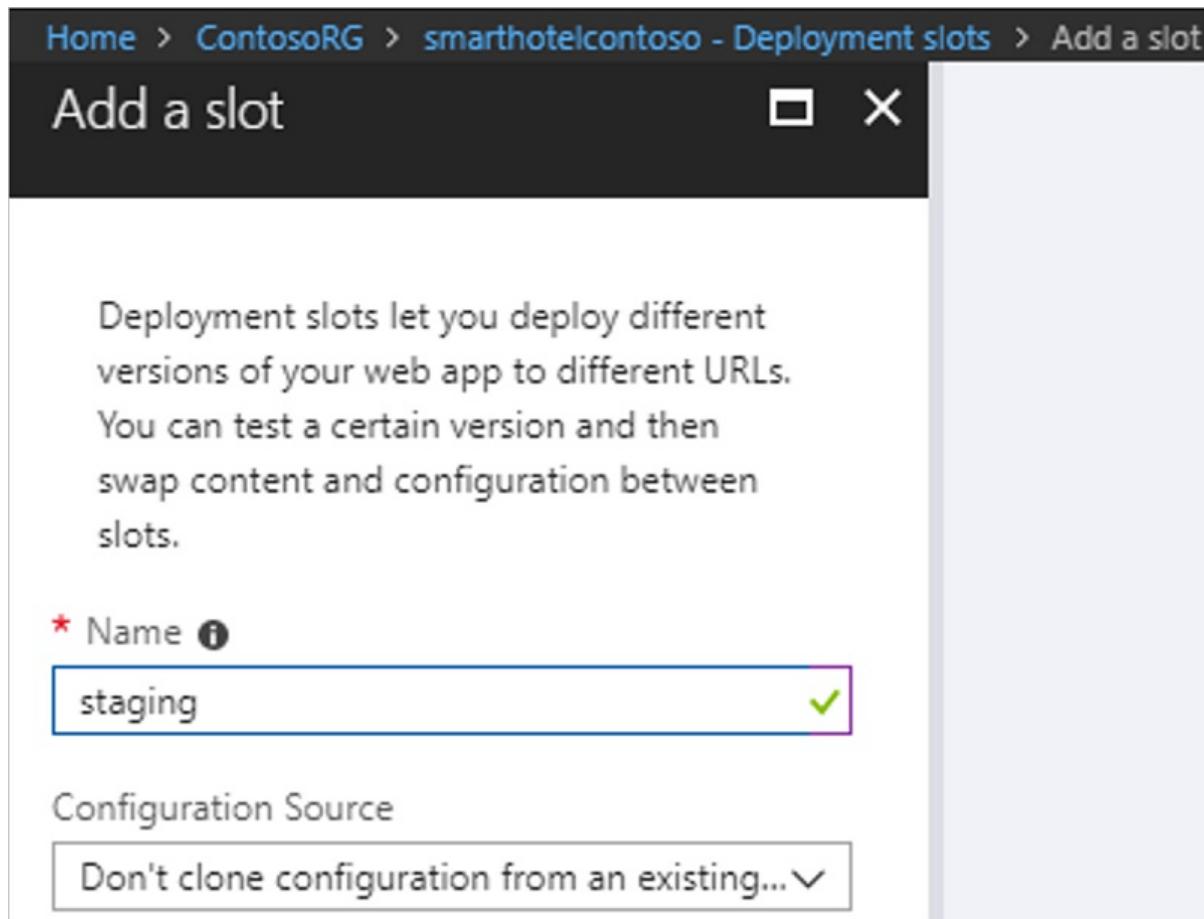


Figure 52: Adding a web app staging slot.

#### Provision the function app

In the Azure portal, Contoso admins provision the function app.

1. They select Function App.

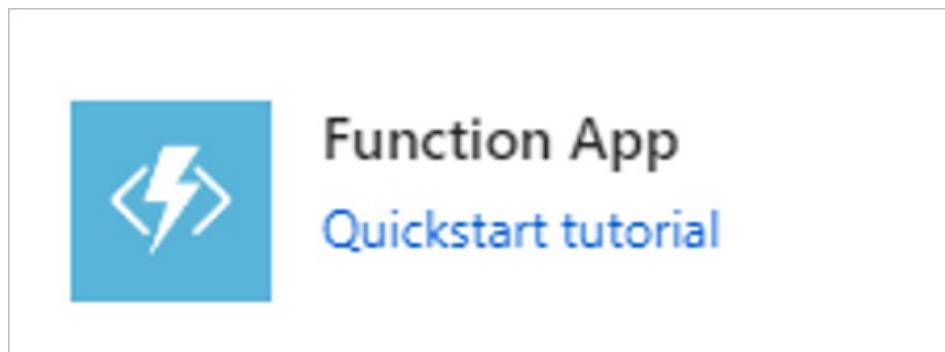


Figure 53: Selecting the function app.

2. They provide a name for the function app (`smarthotelpetchecker`). They place the function app in the production resource group (`ContosoRG`). They set the hosting place to **Consumption Plan**, and place the function app in the `East US 2` region. A new storage account is created along with an Application Insights instance for monitoring.

**Function App**

Create

\* App name  
smarthotelpetchecker

.azurewebsites.net

\* Subscription

\* Resource Group   
 Create new  Use existing

ContosoRG

\* OS Windows Linux (Preview)

\* Hosting Plan   
Consumption Plan

\* Location  
East US 2

\* Storage   
 Create new  Use existing

smarthotelpetchb445

Application Insights On

\* Application Insights Location   
East US

Figure 54: Function app settings.

3. After they've deployed the function app, the admins browse to its address to verify that it has been created successfully.

## Step 4: Set up the front-end pipeline

Contoso admins create two different projects for the front-end site.

1. In Azure DevOps, they create a project `SmartHotelFrontend`.

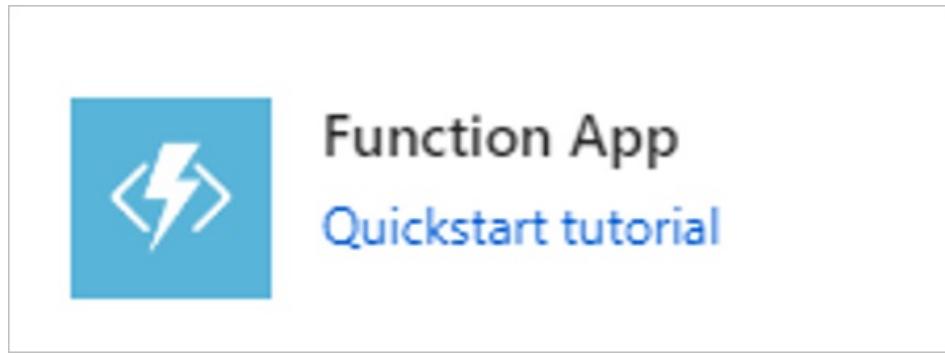


Figure 55: Creating a front-end project.

2. They import the [SmartHotel360 front end](#) Git repository into the new project.
3. For the function app, they create another Azure DevOps project ([SmartHotelPetChecker](#)) and import the [petchecker](#) git repository into this project.

### Configure the web app

Now Contoso admins configure the web app to use Contoso resources.

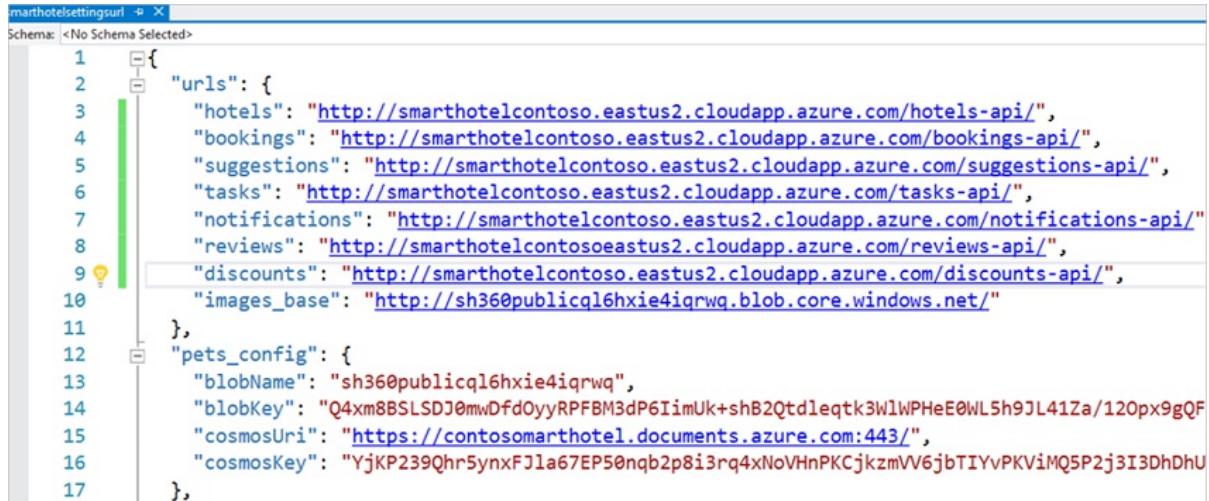
1. The admins connect to the Azure DevOps project and clone the repository locally to the development machine.
2. In Visual Studio, they open the folder to show all the files in the repo.

```
marthotelsettingsurl.json
Schema: <No Schema Selected>
1 {
2   "urls": {
3     "hotels": "http://smarthotelcontoso.eastus2.cloudapp.azure.com/hotels-api/",
4     "bookings": "http://smarthotelcontoso.eastus2.cloudapp.azure.com/bookings-api/",
5     "suggestions": "http://smarthotelcontoso.eastus2.cloudapp.azure.com/suggestions-api/",
6     "tasks": "http://smarthotelcontoso.eastus2.cloudapp.azure.com/tasks-api/",
7     "notifications": "http://smarthotelcontoso.eastus2.cloudapp.azure.com/notifications-api/",
8     "reviews": "http://smarthotelcontoso.eastus2.cloudapp.azure.com/reviews-api/",
9     "discounts": "http://smarthotelcontoso.eastus2.cloudapp.azure.com/discounts-api/",
10    "images_base": "http://sh360publicql6hxie4iqrwq.blob.core.windows.net/"
11  },
12  "pets_config": {
13    "blobName": "sh360publicql6hxie4iqrwq",
14    "blobKey": "Q4xm8BSLSDJ0mwDfdOyyRPFBM3dP6IimUk+shB2Qtdleqtk3W1WPHeE0WL5h9JL41Za/120px9gQF",
15    "cosmosUri": "https://contosomarhotel.documents.azure.com:443/",
16    "cosmosKey": "YjKP239Qhr5ynxFJla67EP50nqb2p8i3rq4xNoVHnPKCjkzmVV6jbTIYvPKViMQ5P2j3I3DhDhu"
17  },
18}
.dockerignore
.gitattributes
.gitignore
.docker-compose.ci.build.yml
.docker-compose.dcproj
.docker-compose.override.yml
.docker-compose.yml
LICENSE
README.md
.SmartHotel360.AzureFunction.sln
.SmartHotel360.PublicWeb.sln
```

Figure 56: Viewing all files in the repo.

3. They update the configuration changes as required.
  - When the web app starts up, it looks for the `SettingsUrl` app setting.
  - This variable must contain a URL that points to a configuration file.

- By default, the setting that's used is a public endpoint.
4. They update the `/config-sample.json/sample.json` file.
- This is the configuration file for the web when it uses the public endpoint.
  - They edit the `urls` and `pets_config` sections with the values for the AKS API endpoints, storage accounts, and Azure Cosmos DB database.
  - The URLs should match the DNS name of the new web app that Contoso will create.
  - For Contoso, this is `smarthotelcontoso.eastus2.cloudapp.azure.com`.



```

1  {
2    "urls": {
3      "hotels": "http://smarthotelcontoso.eastus2.cloudapp.azure.com/hotels-api/",
4      "bookings": "http://smarthotelcontoso.eastus2.cloudapp.azure.com/bookings-api/",
5      "suggestions": "http://smarthotelcontoso.eastus2.cloudapp.azure.com/suggestions-api/",
6      "tasks": "http://smarthotelcontoso.eastus2.cloudapp.azure.com/tasks-api/",
7      "notifications": "http://smarthotelcontoso.eastus2.cloudapp.azure.com/notifications-api/",
8      "reviews": "http://smarthotelcontoso.eastus2.cloudapp.azure.com/reviews-api/",
9      "discounts": "http://smarthotelcontoso.eastus2.cloudapp.azure.com/discounts-api/",
10     "images_base": "http://sh360publicql6hxie4iqrwq.blob.core.windows.net/"
11   },
12   "pets_config": {
13     "blobName": "sh360publicql6hxie4iqrwq",
14     "blobKey": "Q4xm8BSLSDJ0mwDfdOyyRPFBM3dP6IimUk+shB2Qtd1eqtk3WlWPHeE0WL5h9JL41Za/120px9gQF",
15     "cosmosUri": "https://contosomarthotel.documents.azure.com:443/",
16     "cosmosKey": "YjKP239Qhr5ynxFJla67EP50nqb2p8i3rq4xNoVHnPKCjkzmVV6jbTIYvPKViMQ5P2j3I3DhDHU"
17   }
},

```

Figure 57: The json settings.

5. After they update the file, the admins rename it `smarthotelsettingsurl` and upload it to the Blob storage they created earlier.

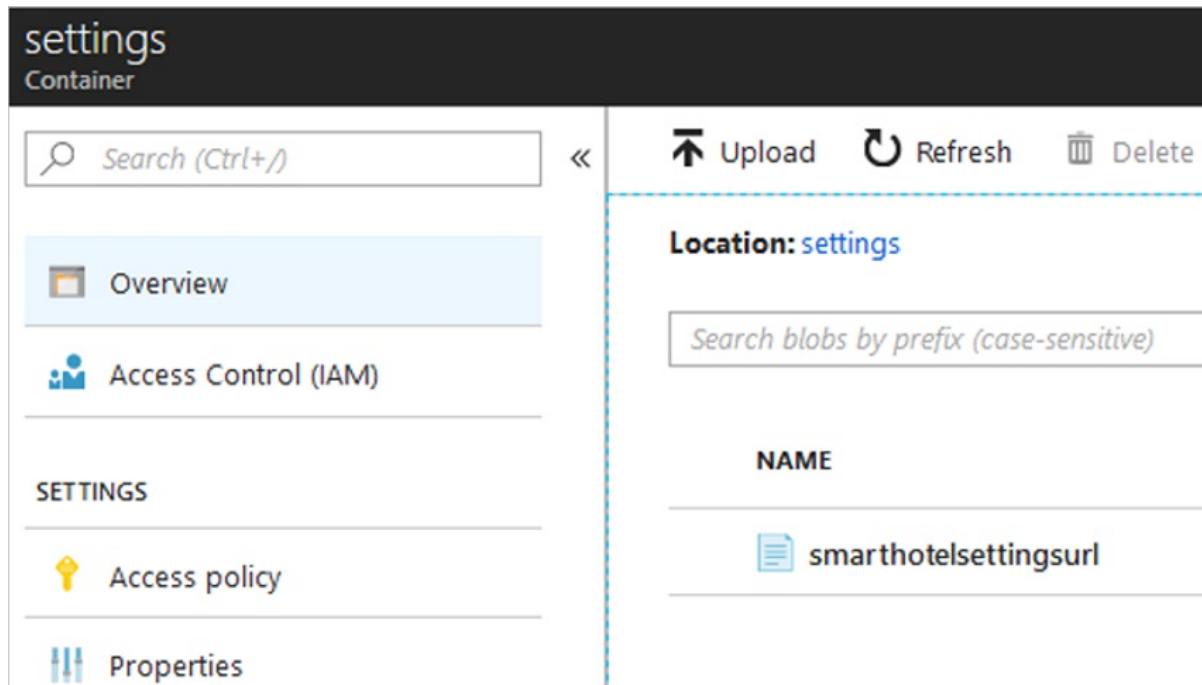


Figure 58: Renaming and uploading the file.

6. They select the file to get the URL. The URL is used by the application when it pulls down the configuration files.

The screenshot shows the Azure Blob storage settings URL page. At the top, there's a header with the title 'smarthotelsettingsurl' and a 'Blob' tab. Below the header are several actions: Save, Discard, Refresh, Download, Acquire lease, and Break lease. A horizontal dashed line separates the header from the main content area. In the main area, there are tabs for Overview, Snapshots, Edit blob, and Generate SAS, with 'Overview' being the active tab. Below the tabs is a section titled 'Properties'. Under 'Properties', there's a 'URL' field containing the value 'https://sh360publicql6hxie4iqrwq.blob.core.windows.net/settings/smarthotelsettingsurl'. To the right of the URL field is a blue icon with a white document symbol, which is highlighted with a red box.

Figure 59: The application URL.

7. In the `appsettings.Production.json` file, they update the `SettingsURL` to the URL of the new file.

The screenshot shows the `appsettings.Production.json` file in a code editor. The schema is defined as `Schema: http://json.schemastore.org/appsettings`. The JSON content is as follows:

```
1 {
2   "Production": true,
3   "SettingsUrl": "https://sh360publicql6hxie4iqrwq.blob.core.windows.net/settings/smarthotelsettingsurl",
```

Figure 60: Updating the URL to the new file.

## Deploy the website to Azure App Service

Contoso admins can now publish the website.

1. They open Azure DevOps and, in the `SmartHotelFrontend` project in **Builds and Releases**, they select **+ New pipeline**.
2. They select **Azure DevOps Git** as a source.
3. They select the **ASP.NET Core** template.
4. They review the pipeline and check to ensure that **Publish Web Projects** and **Zip Published Projects** are selected.

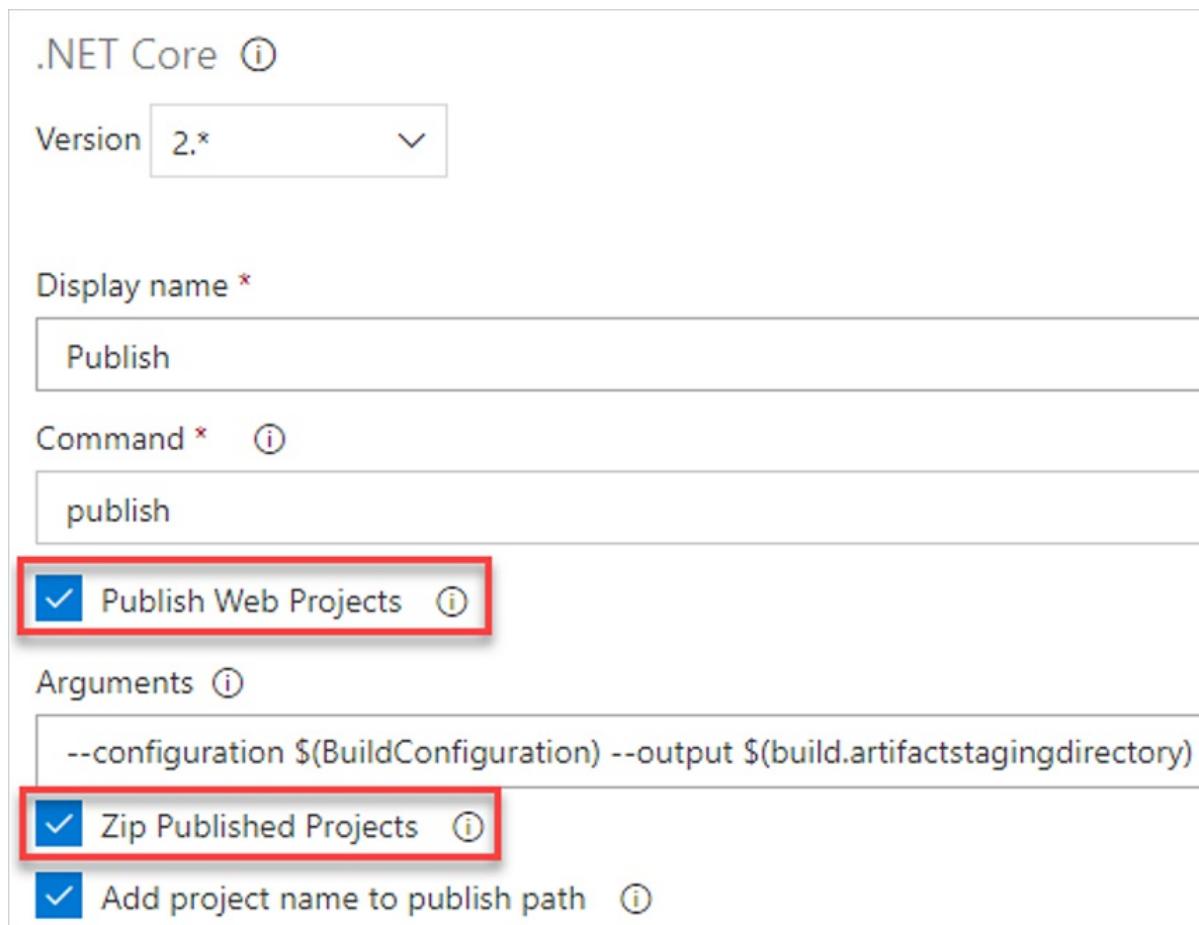


Figure 61: Pipeline settings.

5. In **Triggers**, they enable continuous integration and add the master branch. This ensures that the build pipeline starts each time the solution has new code committed to the master branch.

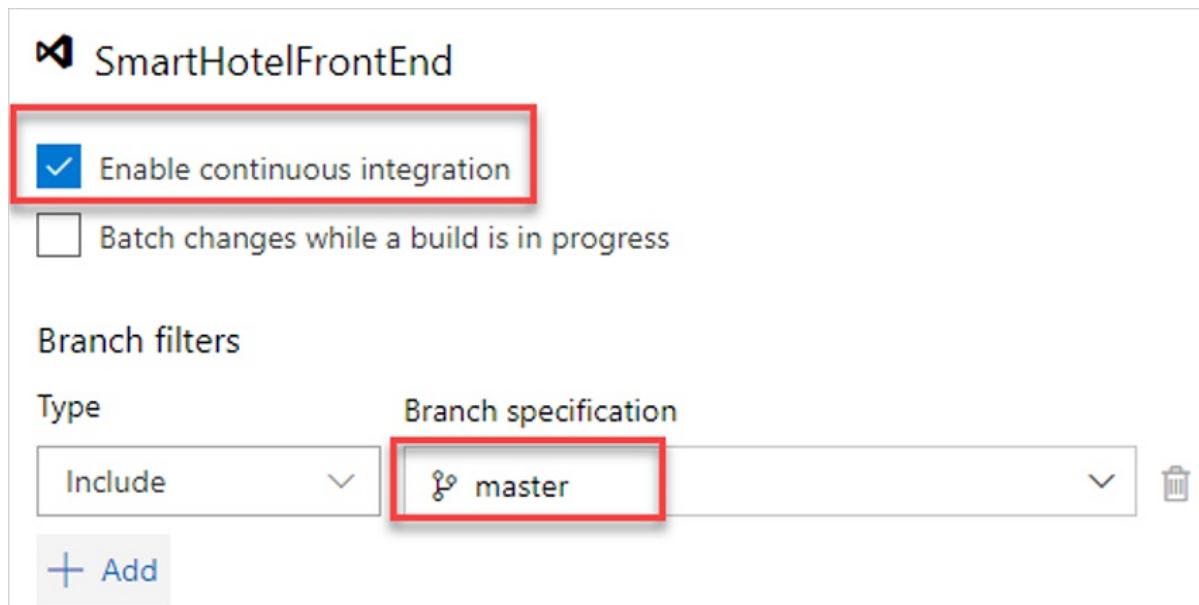


Figure 62: Enabling continuous integration.

6. They select **Save & Queue** to start a build.
7. After the build finishes, they configure a release pipeline by using **Azure App Service Deployment**.
8. They provide a stage name, **Staging**.

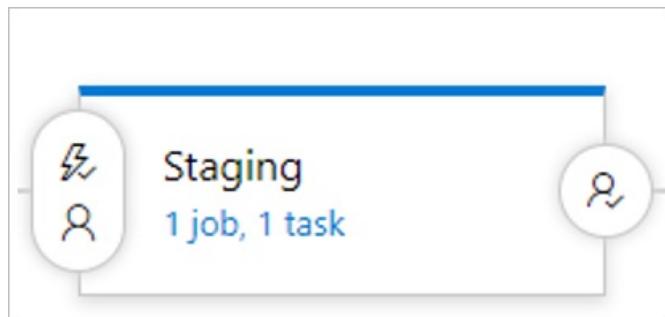


Figure 63: Naming the environment.

9. They add an artifact and select the build that they've configured.

The screenshot shows the 'Add an artifact' configuration page. At the top, it says 'Source type'. Below that, there are three options: 'Build' (selected), 'Git', and 'GitHub'. A red circle highlights the 'Build' icon. Below the source type section, there's a link '4 more artifact types ▾'. Under 'Project \*', the value 'SmartHotelFrontEnd' is listed. Under 'Source (build pipeline) \*', the value 'SmartHotelFrontEnd-ASP.NET Core-CI' is listed, which is also highlighted with a red rectangle.

Figure 64: Adding an artifact.

10. They select the lightning bolt icon on the artifact and then set continuous deployment to Enabled.

## Continuous deployment trigger

Build: \_SmartHotelFrontEnd-ASP.NET Core-CI



Creates release every time a new build is available.

Figure 65: Enabling continuous deployment.

11. In Environment, they select 1 job, 1 task under Staging.
12. After selecting the subscription and web app name, the admins open the Deploy Azure App Service task. The deployment is configured to use the **staging** deployment slot. This automatically builds code for review and approval in this slot.

## Azure App Service Deploy ⓘ

Version 3.\* ▾

Display name \*

Azure App Service Deploy: smarhotelcontoso

Azure subscription \* ⚙ | Manage ↗

|

App type \* ⓘ

Web App

App Service name \* ⚙

smarhotelcontoso



Deploy to slot ⓘ

Resource group \* ⓘ

ContosoRG

Slot \* ⓘ

staging

Figure 66: Deploying to a slot.

13. In the Pipeline, they add a new stage.

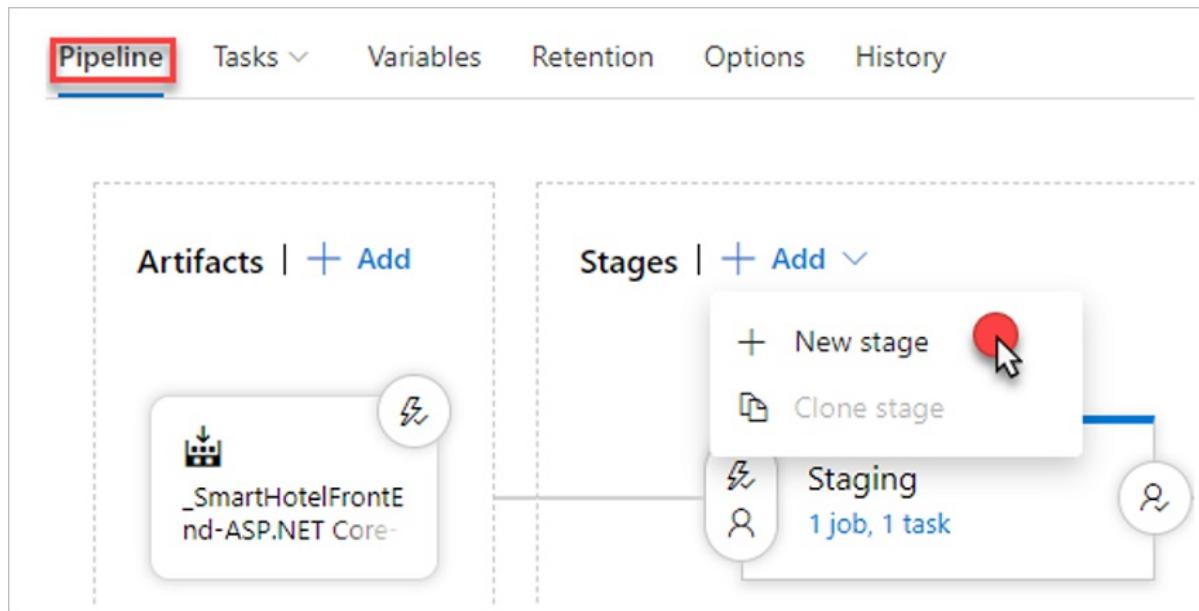


Figure 67: Adding a new stage.

14. They select **Azure App Service deployment with slot** and then name the environment **Prod**.
15. They select **1 job, 2 tasks** and then select the subscription, the app service name, and the **staging** slot.

Environment name

Prod

Parameters ⓘ | ⚙️ Unlink all

Azure subscription \* 🔗 | Manage ↗

App type 🔗

Web App

App service name \* 🔗

smarthotelcontoso

Deploy to slot 🔗

Resource group \* 🔗

ContosoRG

Slot \* 🔗

staging

Figure 68: Naming the environment.

16. They remove the Deploy Azure App Service to Slot from the pipeline. It was placed there by the previous steps.

Azure App Service Manage ⓘ

Version 0.\* ▾

Display name \*

Manage Azure App Service - Slot Swap

Azure subscription \* ⚙ | Manage ↗

Action ⓘ

Swap Slots

App Service name \* ⚙

smarthotelcontoso

Resource group \* ⚙

ContosoRG

Source Slot \* ⚙

staging

Swap with Production ⓘ

Figure 69: Removing a slot from the pipeline.

17. They save the pipeline. On the pipeline, they select Post-deployment conditions.

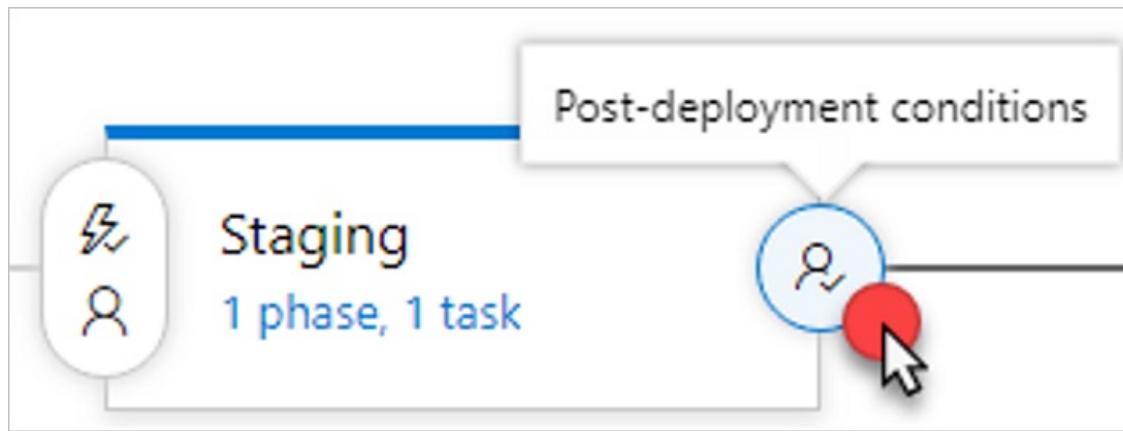


Figure 70: Post-deployment conditions.

18. They enable Post-deployment approvals and then add a dev lead as the approver.

The screenshot shows the 'Post-deployment conditions' settings for the 'Staging' environment. It includes a section for 'Post-deployment approvals' which is currently 'Enabled'. Below this, there's a search bar labeled 'Search users and groups' with a placeholder 'X' and a small user profile icon.

Figure 71: Adding an approver.

19. In the build pipeline, the admins manually kick off a build. This triggers the new release pipeline, which deploys the site to the staging slot. For Contoso, the URL for the slot is

`https://smarthotelcontoso-staging.azurewebsites.net/`

20. After the build finishes and the release is deployed to the slot, Azure DevOps emails the dev lead for approval.

21. The dev lead selects **View approval** and can approve or reject the request in the Azure DevOps portal.

The screenshot shows the 'SmartHotelFrontendRelease / Release-1' pipeline summary. At the top, there's a navigation bar with tabs for 'Summary', 'Environments', 'Artifacts', 'Variables', 'General', 'Commits', 'Work items', 'Tests', 'Logs', and 'History'. Below the navigation bar, there are buttons for 'Deploy', 'Save', 'Abandon', 'Release (pipeline view)', and 'Send Email'. A yellow banner at the bottom states 'A post-deployment approval is pending for the 'Staging' environment.' with a red box around the 'Approve or reject' link.

Figure 72: A pending release approval request.

22. The dev lead makes a comment and approves. This starts swapping the **staging** and **prod** slots and moves the build into production.

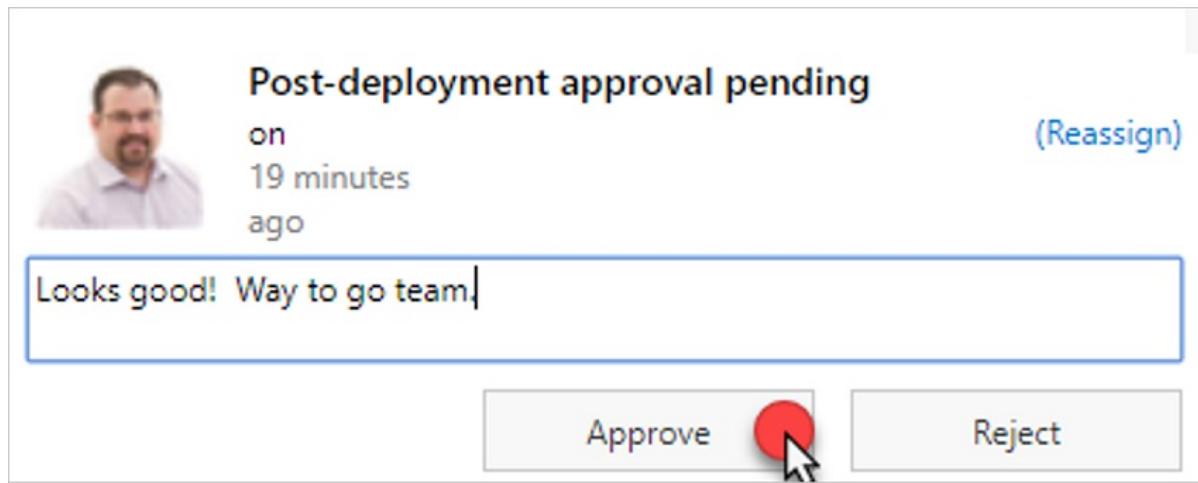


Figure 73: Moving the build into production.

23. The pipeline completes the swap.

Environments				
Environment	Actions	Deployment status	Triggered	Completed
Staging	...	SUCCEEDED	22 minutes ago	just now
Prod	...	IN PROGRESS	just now	

Figure 74: Completing the swap.

24. The team checks the **prod** slot to verify that the web app is in production at

<https://smarthotelcontoso.azurewebsites.net/>.

### Deploy the PetChecker function app

Contoso admins deploy the application by doing the following:

1. They clone the repository locally to the development machine by connecting to the Azure DevOps project.
2. In Visual Studio, they open the folder to show all the files in the repo.
3. They open the `src/PetCheckerFunction/local.settings.json` file and add the app settings for storage, the Azure Cosmos DB database, and the Computer Vision API.

```
local.settings.json ✘ X
Schema: <No Schema Selected>
1 {
2   "IsEncrypted": false,
3   "Values": {
4     "AzureWebJobsStorage": "DefaultEndpointsProtocol=https;AccountName=sh360publicql6hxie4i",
5     "AzureWebJobsDashboard": "",
6     "cosmos_uri": "https://contososmarthotel.documents.azure.com:443/",
7     "cosmos_key": "umxedYGmD3JNvFs1Az0yuxR77BX8k2BjTF7cJBshYMAhZNSr3sTtsuEl4kKG4zpqsVWaE1",
8     "constr": "AccountEndpoint=https://contososmarthotel.documents.azure.com:443/;AccountKe",
9     "MicrosoftVisionApiKey": "fa7a5a7fed1745bfa8cc242f0a9cd2f0",
10    "MicrosoftVisionApiEndpoint": "https://eastus2.api.cognitive.microsoft.com/vision/v1.0",
11    "MicrosoftVisionNumTags": "10"
12  }
13 }
```

Figure 75: Deploying the function.

4. They commit the code and sync it back to Azure DevOps, pushing their changes.
5. They add a new build pipeline and then select **Azure DevOps Git** for the source.
6. They select the **ASP.NET Core (.NET Framework)** template.

7. They accept the defaults for the template.
8. Under Triggers, they select **Enable continuous integration** and then select **Save & Queue** to start a build.
9. After the build succeeds, they build a release pipeline, adding **Azure App Service deployment with slot**.
10. They name the environment **Prod** and then select the subscription. They set the **App type** to **Function App** and the app service name as `smarthotelpetchecker`.

**Environment name**

Prod

**Parameters** ⓘ | ⚙️ [Unlink all](#)

Azure subscription \* ⚙️ | [Manage](#) ↗

This field is linked to 1 setting in 'Deploy Azure App Service'

App type ⚙️

Function App

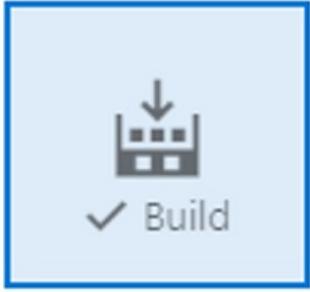
App service name \* ⚙️

smarthotelpetchecker

Figure 76: The function app.

11. They add an artifact, **Build**.

Source type

 Build

 Git

 GitHub

[4 more artifact types ▾](#)

Project \* (i)

SmartHotelPetChecker

Source (build pipeline) \* (i)

SmartHotelPetChecker-ASP.NET Core (.NET Framework)-CI

Default version \* (i)

Latest

Figure 77: Adding an artifact.

12. They enable **Continuous deployment trigger** and then select **Save**.
13. They select **Queue new build** to run the full CI/CD pipeline.
14. After the function is deployed, it appears in the Azure portal with the status **Running**.

Home > App Services > smarthotelpetchecker

## smarthotelpetchecker

Function Apps

Search

All subscriptions

Function Apps

smarthotelpetchecker

Functions (Read Only)

PetChecker

Overview

Stop Swap

Status

Running

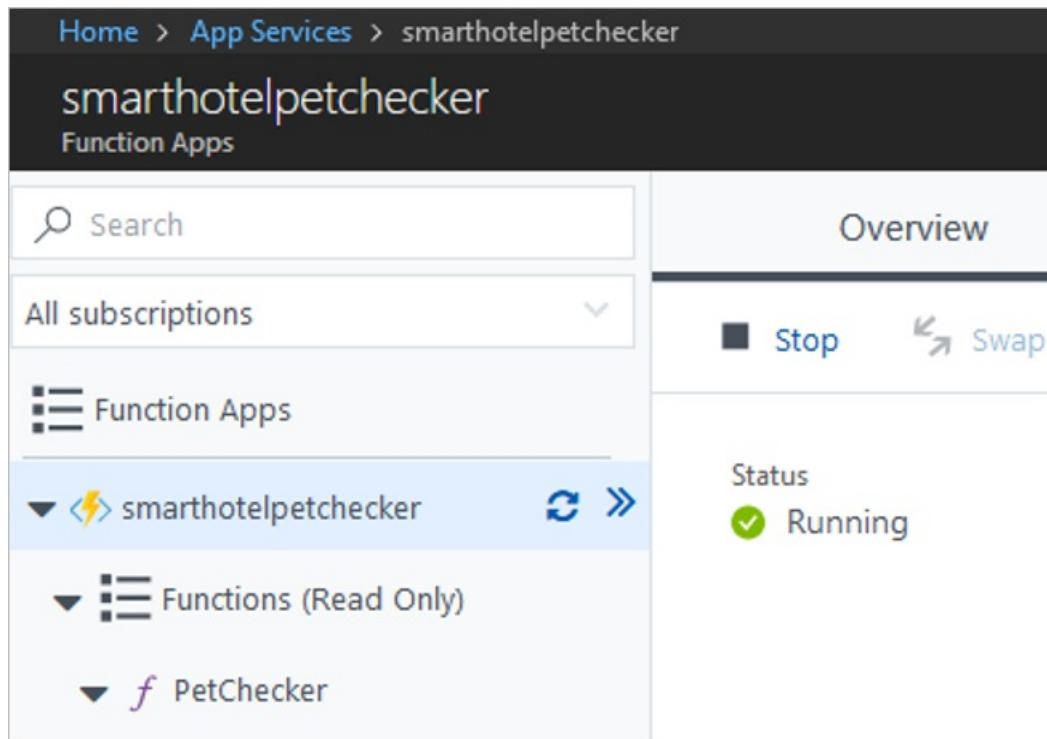


Figure 78: Updating the function's status.

15. They browse to the pet checker application, at <http://smarthotel360public.azurewebsites.net/pets>, to verify that it's working properly.
16. They select the avatar to upload a picture.

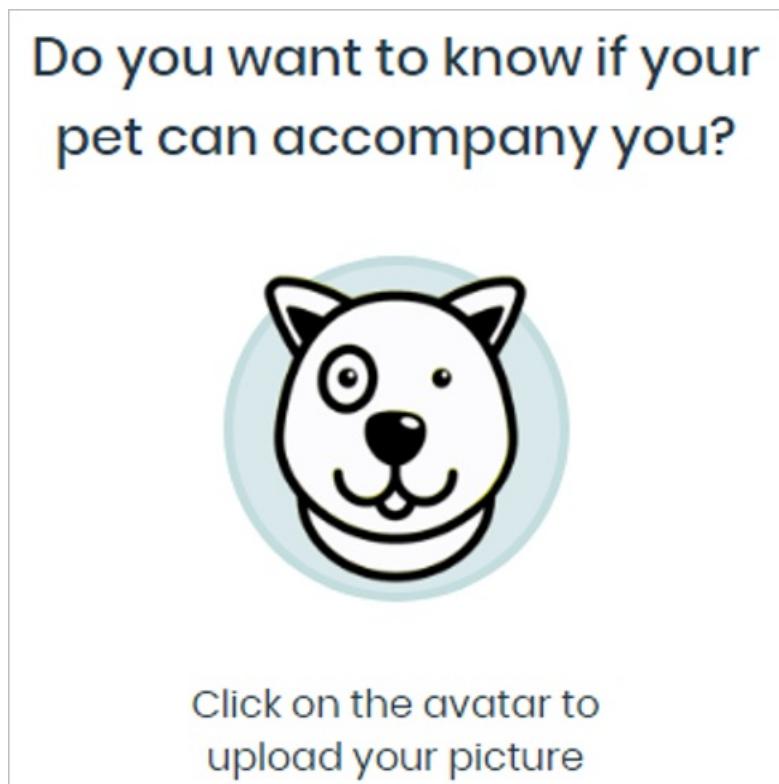


Figure 79: Assigning a picture to an avatar.

17. The first photo they want to check is of a small dog.

Do you want to know if your pet can accompany you?



Processing the image...

Figure 80: Checking the photo.

18. The application returns an acceptance message.

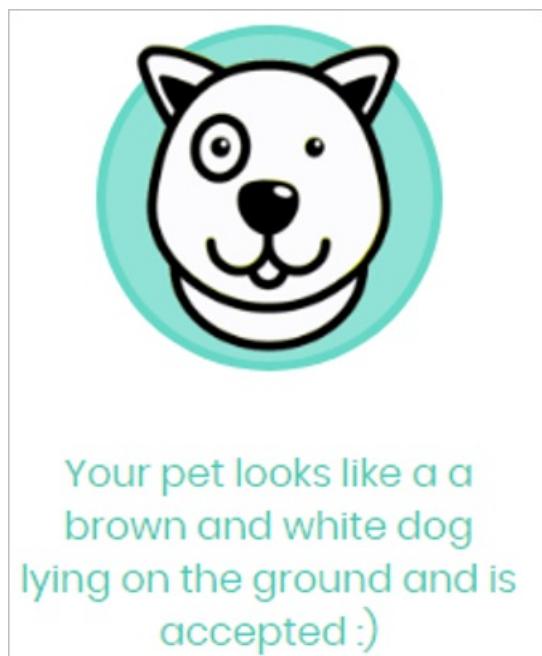


Figure 81: An acceptance message.

## Review the deployment

With the migrated resources in Azure, Contoso now needs to fully operationalize and secure the new infrastructure.

### Security

- Contoso needs to ensure that the new databases are secure. To learn more, see [Overview of Azure SQL Database and SQL Managed Instance security capabilities](#).
- The application must be updated to use SSL with certificates. The container instance should be redeployed to answer on 443.
- Contoso should consider using Azure Key Vault to help protect secrets for their Service Fabric applications. To learn more, see [Manage encrypted secrets in Service Fabric applications](#).

### Backups and disaster recovery

- Contoso needs to review [backup requirements for Azure SQL Database](#).
- Contoso should consider implementing [SQL failover groups to provide regional failover for the database](#).
- Contoso can use [geo-replication for the Azure Container Registry Premium SKU](#).
- Azure Cosmos DB is backed up automatically. To learn more, see [Online backup and on-demand data restore in Azure Cosmos DB](#).

Azure Cosmos DB.

### Licensing and cost optimization

- After all resources are deployed, Contoso should assign Azure tags based on their [infrastructure planning](#).
- All licensing is built into the cost of the PaaS services that Contoso is consuming. This will be deducted from the Enterprise Agreement.
- Contoso will enable [Azure Cost Management + Billing](#) to help monitor and manage the Azure resources.

## Conclusion

In this article, Contoso rebuilds the SmartHotel360 application in Azure. The on-premises application front-end VM is rebuilt for Azure App Service web apps. The application back end is built by using microservices that are deployed to containers managed by AKS. Contoso enhanced functionality with a pet photo application.

## Suggested skills

Microsoft Learn is a new approach to learning. Readiness for the new skills and responsibilities that come with cloud adoption doesn't come easily. Microsoft Learn provides a more rewarding approach to hands-on learning that helps you achieve your goals faster. With Microsoft Learn, you can earn points, rise through levels, and achieve more.

Here are two examples of tailored learning paths on Microsoft Learn that align with the Contoso SmartHotel360 application in Azure.

- **[Deploy a website to Azure with Azure App Service](#)**: By creating web apps in Azure, you can publish and manage your website easily without having to work with the underlying servers, storage, or network assets. Instead, you can focus on your website features and rely on the robust Azure platform to help provide secure access to your site.
- **[Process and classify images with the Azure Cognitive Vision Services](#)**: Azure Cognitive Services offers prebuilt functionality to enable computer vision functionality in your applications. Learn how to use the Azure Cognitive Vision Services to detect faces, tag and classify images, and identify objects.

# Refactor a Team Foundation Server deployment to Azure DevOps Services

11/9/2020 • 17 minutes to read • [Edit Online](#)

This article shows how the fictional company Contoso refactors its on-premises Visual Studio Team Foundation Server deployment by migrating it to Azure DevOps Services in Azure. The Contoso development team has used Team Foundation Server for team collaboration and source control for the past five years. Now, the team wants to move to a cloud-based solution for dev and test work and for source control. Azure DevOps Services will play a role as the Contoso team moves to an Azure DevOps model and develops new cloud-native applications.

## Business drivers

The Contoso IT leadership team has worked closely with business partners to identify future goals. The partners aren't overly concerned with dev tools and technologies, but the team has captured these points:

- **Software:** Regardless of the core business, all companies are now software companies, including Contoso. Business leadership is interested in how IT can help lead the company with new working practices for users and new experiences for its customers.
- **Efficiency:** Contoso needs to streamline its processes and remove unnecessary procedures for developers and users. Doing so will allow the company to deliver on customer requirements more efficiently. The business needs IT to move quickly, without wasting time or money.
- **Agility:** To enable its success in a global economy, Contoso IT needs to be more responsive to the needs of the business. It must be able to react more quickly to changes in the marketplace. IT must not get in the way or become a business blocker.

## Migration goals

The Contoso cloud team has pinned down the following goals for its migration to Azure DevOps Services:

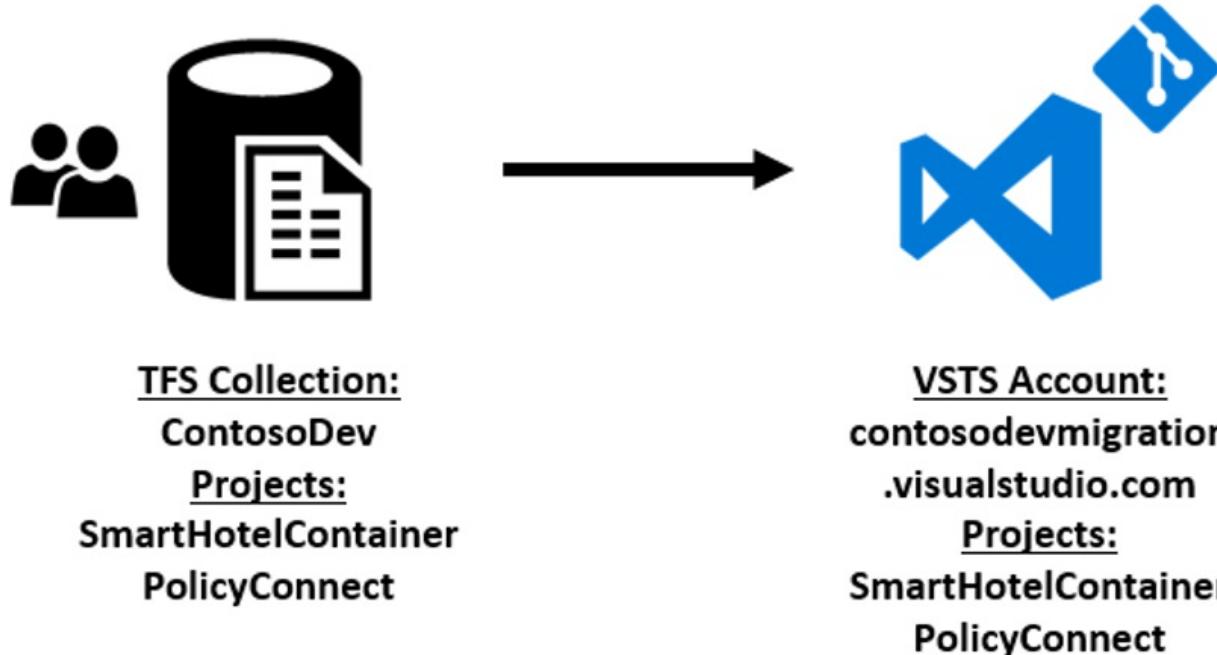
- The team needs a tool to migrate its data to the cloud. Few manual processes should be needed.
- Work item data and history for the last year must be migrated.
- The team doesn't want to set up new user names and passwords. All current system assignments must be maintained.
- The team wants to move away from Team Foundation Version Control (TFVC) to Git for source control.
- The transition to Git will be a tip migration that imports only the latest version of the source code. The transition will happen during a downtime, when all work will be halted as the code base shifts. The team understands that only the current master branch history will be available after the move.
- The team is concerned about the change and wants to test it before it does a full move. The team wants to retain access to Team Foundation Server even after the move to Azure DevOps Services.
- The team has multiple collections and, to better understand the process, it wants to start with one that has only a few projects.
- The team understands that Team Foundation Server collections are a one-to-one relationship with Azure DevOps Services organizations, so it will have multiple URLs. But this matches its current model of separation for code bases and projects.

## Proposed architecture

- Contoso will move its Team Foundation Server projects to the cloud, and it will no longer host its projects or

source control on-premises.

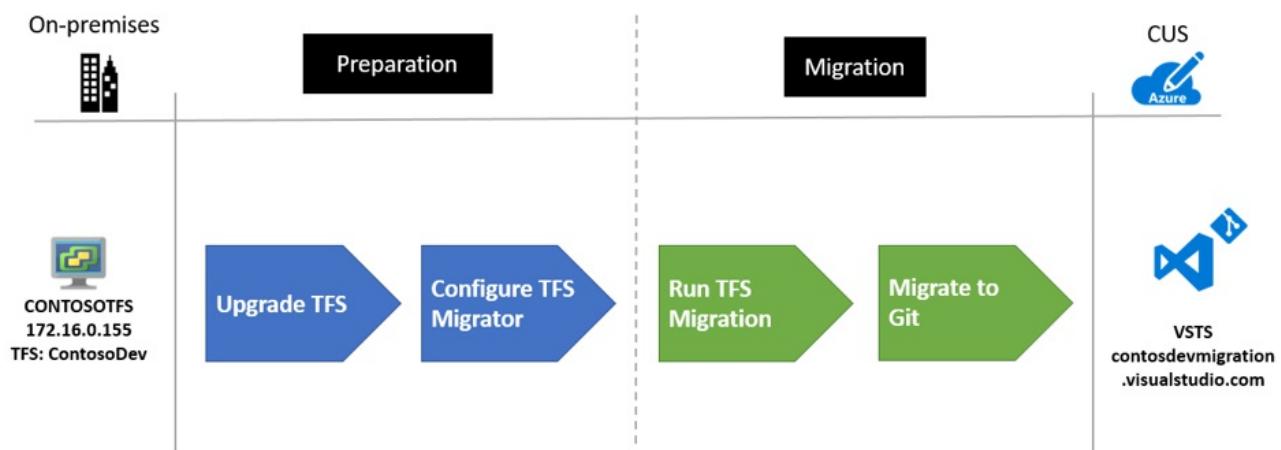
- Team Foundation Server will be migrated to Azure DevOps Services.
- Currently, Contoso has one Team Foundation Server collection, named `ContosoDev`, which will be migrated to an Azure DevOps Services organization called `contosodevmigration.visualstudio.com`.
- The projects, work items, bugs, and iterations from the last year will be migrated to Azure DevOps Services.
- Contoso will use its Azure Active Directory (Azure AD) instance, which it set up when it [deployed its Azure infrastructure](#) at the beginning of the migration planning.



## Migration process

Contoso will complete the migration process as follows:

1. Significant preparation is required. First, Contoso must upgrade its Team Foundation Server implementation to a supported level. Contoso is currently running Team Foundation Server 2017 Update 3, but to use database migration it needs to run a supported 2018 version with the latest updates.
2. After Contoso upgrades, it will run the Team Foundation Server migration tool and validate its collection.
3. Contoso will build a set of preparation files and then perform a migration dry run for testing.
4. Contoso will then run another migration, this time a full migration that includes work items, bugs, sprints, and code.
5. After the migration, Contoso will move its code from TFVC to Git.



# Prerequisites

To run this scenario, Contoso needs to meet the following prerequisites:

Requirements	Details
Azure subscription	<p>Contoso created subscriptions in an earlier article in this series. If you don't have an Azure subscription, create a <a href="#">free account</a>.</p> <p>If you create a free account, you're the administrator of your subscription and can perform all actions.</p> <p>If you use an existing subscription and you're not the administrator, you need to work with the admin to assign you Owner or Contributor permissions.</p> <p>If you need more granular permissions, see <a href="#">Manage Site Recovery access with role-based access control (RBAC)</a>.</p>
Azure infrastructure	Contoso set up its Azure infrastructure as described in <a href="#">Azure infrastructure for migration</a> .
On-premises Team Foundation Server instance	The on-premises instance needs to either run Team Foundation Server 2018 upgrade 2 or be upgraded to it as part of this process.

## Scenario steps

Here's how Contoso will complete the migration:

- **Step 1: Create an Azure storage account.** This storage account will be used during the migration process.
- **Step 2: Upgrade Team Foundation Server.** Contoso will upgrade its deployment to Team Foundation Server 2018 upgrade 2.
- **Step 3: Validate the Team Foundation Server collection.** Contoso will validate the Team Foundation Server collection in preparation for the migration.
- **Step 4: Build the migration files.** Contoso will create the migration files by using the Team Foundation Server migration tool.

## Step 1: Create an Azure storage account

1. In the Azure portal, Contoso admins create a storage account (`contosodevmigration`).
2. They place the account in the secondary region, which they use for failover (`Central US`). They use a general-purpose standard account with locally redundant storage.

Create storage account □ X

The cost of your storage account depends on the usage and the options you choose below.

[Learn more](#)

**\* Name** i  
contosodevmigration ✓  
.core.windows.net

**Deployment model** i  
**Resource manager** Classic

**Account kind** i  
Storage (general purpose v1) ▼

**\* Location**  
Central US ▼

**Replication** i  
Locally-redundant storage (LRS) ▼

**Performance** i  
**Standard** Premium

#### Need more help?

- [Introduction to Azure Storage.](#)
- [Create a storage account.](#)

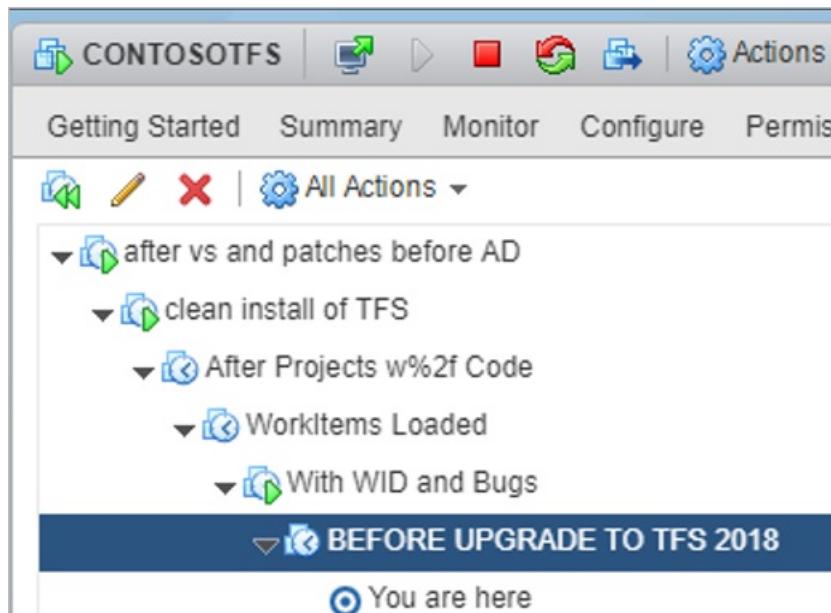
## Step 2: Upgrade Team Foundation Server

Contoso admins upgrade the Team Foundation Server instance to Team Foundation Server 2018 Update 2. Before they start, they:

- Download [Team Foundation Server 2018 Update 2](#).
- Verify the [hardware requirements](#).
- Read the [release notes](#) and [upgrade gotchas](#).

They upgrade as follows:

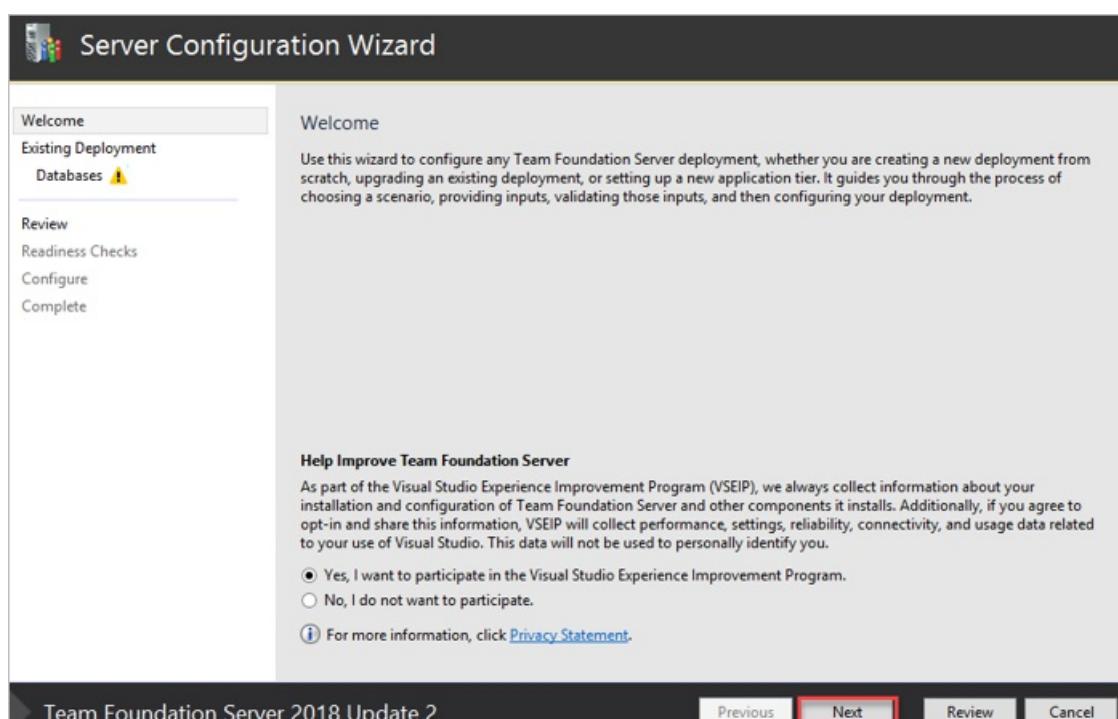
1. To start, the admins back up their Team Foundation Server instance, which is running on a VMware virtual machine (VM), and they take a VMware snapshot.



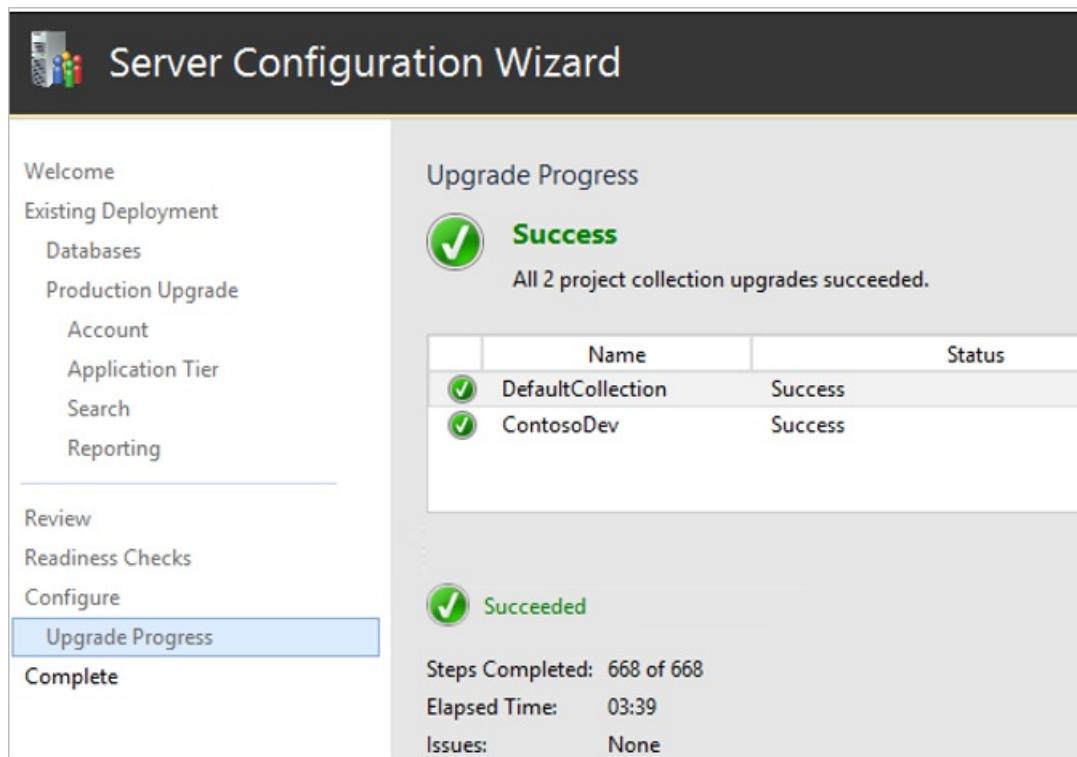
2. The Team Foundation Server installer starts, and they choose the installation location. The installer needs internet access.



3. After the installation finishes, the Server Configuration Wizard starts.



4. After verification, the Server Configuration Wizard completes the upgrade.



5. The admins verify the Team Foundation Server installation by reviewing projects, work items, and code.

The screenshot shows the 'Project Overview - Microsoft' interface. The URL in the address bar is `contosotsf:8080/tfs/ContosoDev/PolicyConnect/_backlogs?level=Epics&_a=backlog`. The top navigation bar includes links for Apps, Projects - Microsoft, PolicyConnect, and SmartHotel. The main menu has tabs for Backlogs and Queries, with Backlogs selected. The left sidebar shows categories: Epics, Features, Backlog items, Past, Current, and Sprint 6. The main content area is titled 'Product backlog' and shows a table of work items:

Order	Work Item Type	Title
1	Epic	2018 - Q2 - Initiatives
+ (highlighted)	Feature	Q2 - Feature 4
	Product Backl...	Q2 - Feature 4 - PBI - 1
	Product Backl...	Q2 - Feature 4 - PBI - 2
	Product Backl...	Q2 - Feature 4 - PBI - 3
	Product Backl...	Q2 - Feature 4 - PBI - 4
	Product Backl...	Q2 - Feature 4 - PBI - 5
	Product Backl...	Q2 - Feature 4 - PBI - 6
	Product Backl...	Q2 - Feature 4 - PBI - 7
	Product Backl...	Q2 - Feature 4 - PBI - 8
	Product Backl...	Q2 - Feature 4 - PBI - 9
	Product Backl...	Q2 - Feature 4 - PBI - 10

#### NOTE

Some Team Foundation Server upgrades need to run the Configure Features wizard after the upgrade finishes. [Learn more.](#)

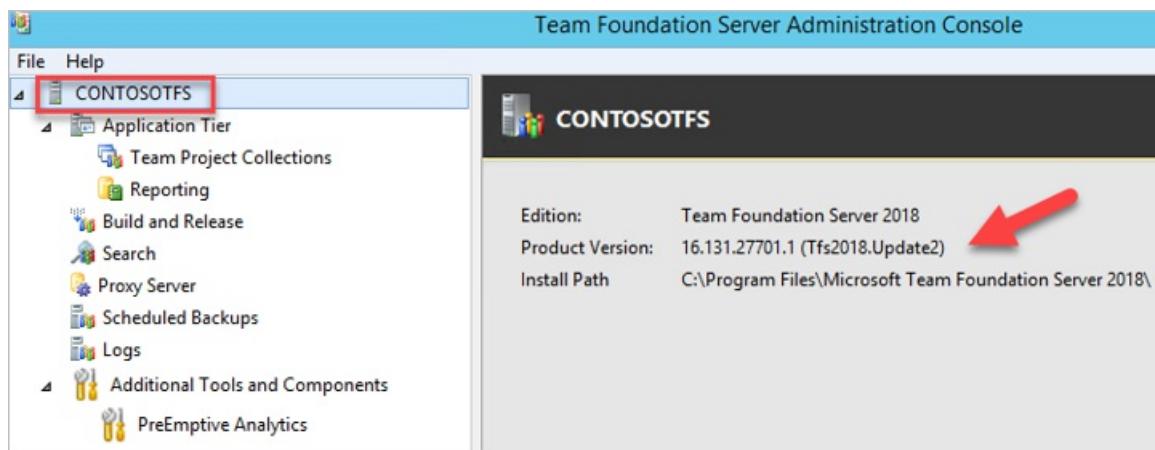
Need more help?

Learn about [upgrading Team Foundation Server](#).

## Step 3: Validate the Team Foundation Server collection

Contoso admins run the Team Foundation Server migration tool against the `contosodev` collection database to validate it before migration.

1. They download and unzip the [Team Foundation Server migration tool](#). It's important to download the version for the Team Foundation Server update that's running. The version can be checked in the admin console.



## Choose the download you want

The screenshot shows a list of download options:

- File Name
- TFS to VSTS Cloud Migration Guide.pdf
- TfsMigrator\_Tfs2018\_Update1\_16.123.5270794.zip
- TfsMigrator\_Tfs2018\_Update2\_16.131.6131836.zip

2. They run the tool to perform the validation by specifying the URL of the project collection, as shown in the following command:

```
TfsMigrator validate /collection:http://contosotfs:8080/tfs/ContosoDev
```

The tool shows an error.

```

-----  

Validating ContosoDev (id = 5f815a1b-c82e-4684-918f-5d368dad733a)  

-----  

Validating that the collection is OK to be imported...  

Validating Collection Metadata      Passed (Step 15 of 15)  

Validating Project Processes       Passed (Validating Project 2 of 2)  

Collection validation completed.  

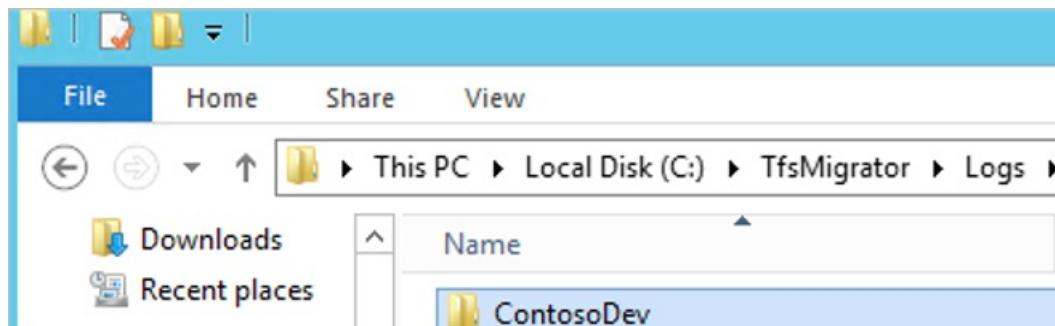
Results:  

+ All collection validations completed with the following errors:  

+ [Error] Errors encountered during identity validation, please review the logs for more details.

```

3. They locate the log files in the `Logs` folder, just before the tool location. A log file is generated for each major validation. `TfsMigration.log` holds the main information.



4. They find this entry, which is related to identity.

```

Identity Validation failed, please provide a TenantDomainName
Validation completed 'Validate Identities' with result Failed, message Errors encountered during identity validation

```

5. They run `TfsMigrator validate /help` at the command line, and they see that the command `/tenantDomainName` seems to be required to validate identities.

```

-----  

Tenant Domain Name  

-----  

The tenant domain specifies the directory to use when validating your Identities list in the import.json  

/tenantDomainName:name - Name of a AAD domain.

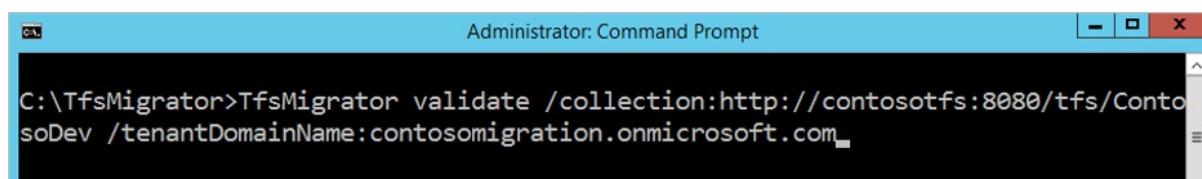
```

6. They run the validation command again and include this value and their Azure AD name,

```

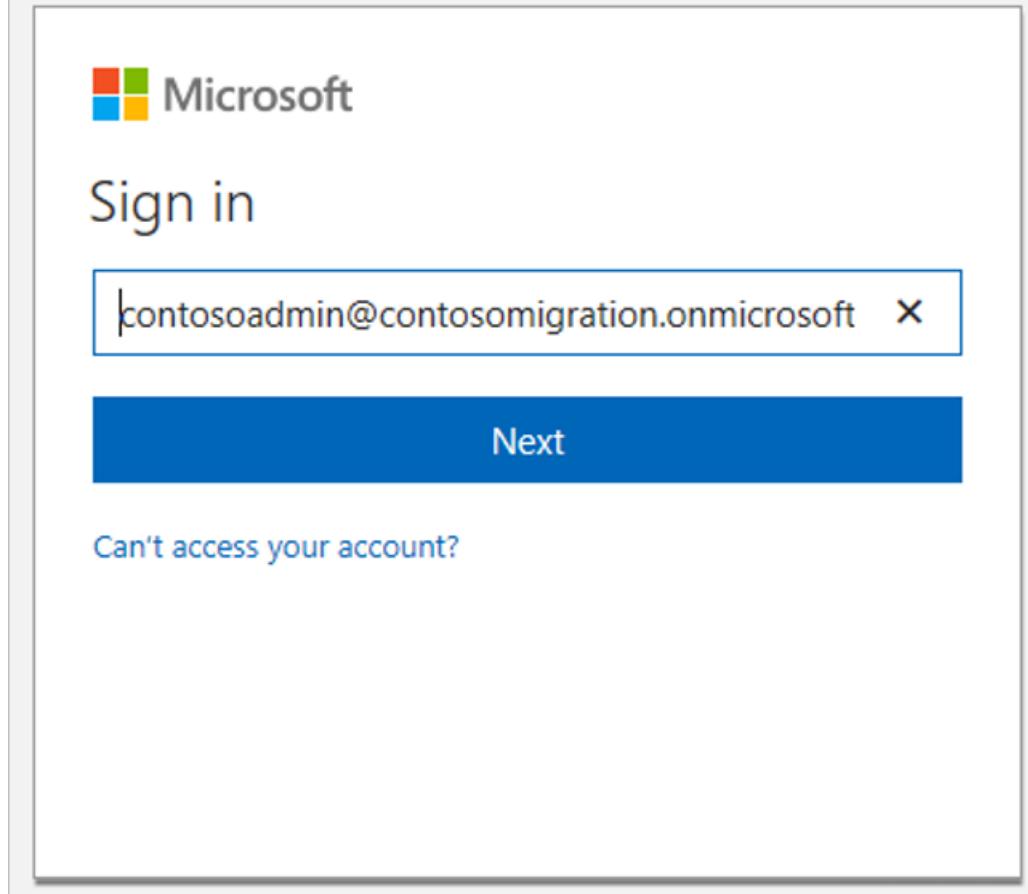
TfsMigrator validate /collection:http://contosotfs:8080/tfs/ContosoDev
/tenantDomainName:contosomigration.onmicrosoft.com

```



7. In the Azure AD sign-in window that opens, they enter the credentials of a global admin user.

# Microsoft Azure



8. The validation passes and is confirmed by the tool.

```
-----  
Guidance  
-----  
  
Collection validation was successful. Recommended next steps:  
  
1) If you haven't run Prepare, next you'll need to generate import files  
2) See TfsMigrator Prepare /help for guidance on how to run the command  
3) If you've run prepare and made changes to the generated files be sure to re-validate them  
4) See TfsMigrator Validate /help for details on re-validating import files
```

## Step 4: Build the migration files

With the validation complete, Contoso admins can use the Team Foundation Server migration tool to build the migration files.

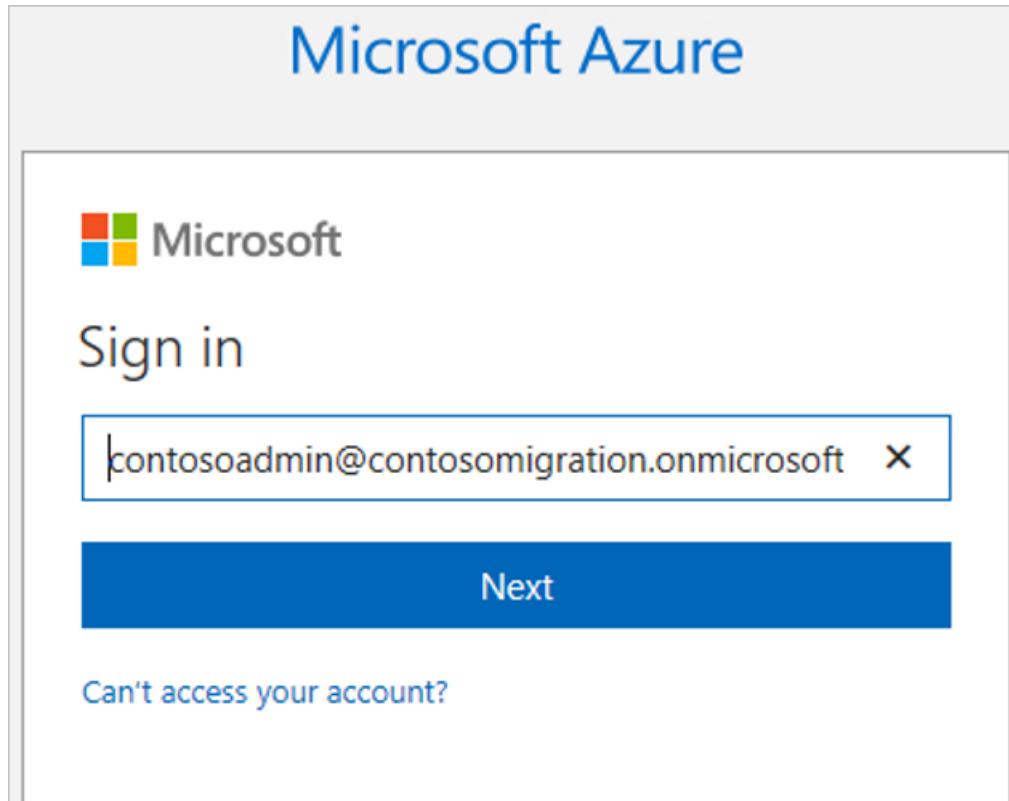
1. They run the preparation step in the tool.

```
TfsMigrator prepare /collection:http://contosotfs:8080/tfs/ContosoDev  
/tenantDomainName:contosomigration.onmicrosoft.com /accountRegion:cus
```

The screenshot shows a Windows Command Prompt window. The title bar says "Administrator: Command Prompt". The main window shows the command "TfsMigrator prepare /collection:http://contosotfs:8080/tfs/ContosoDev /tenantDomainName:contosomigration.onmicrosoft.com /accountRegion:cus" being typed in.

The preparation step does the following:

- Scans the collection to find a list of all users and then populates the identify map log (`IdentityMapLog.csv`).
  - Prepares the connection to Azure AD to find a match for each identity.
  - Contoso has already deployed Azure AD and synchronized it by using Azure AD Connect, so the prepare command should be able to find the matching identities and mark them as **Active**.
2. An Azure AD sign-in screen appears, and the admins enter the credentials of a global admin.



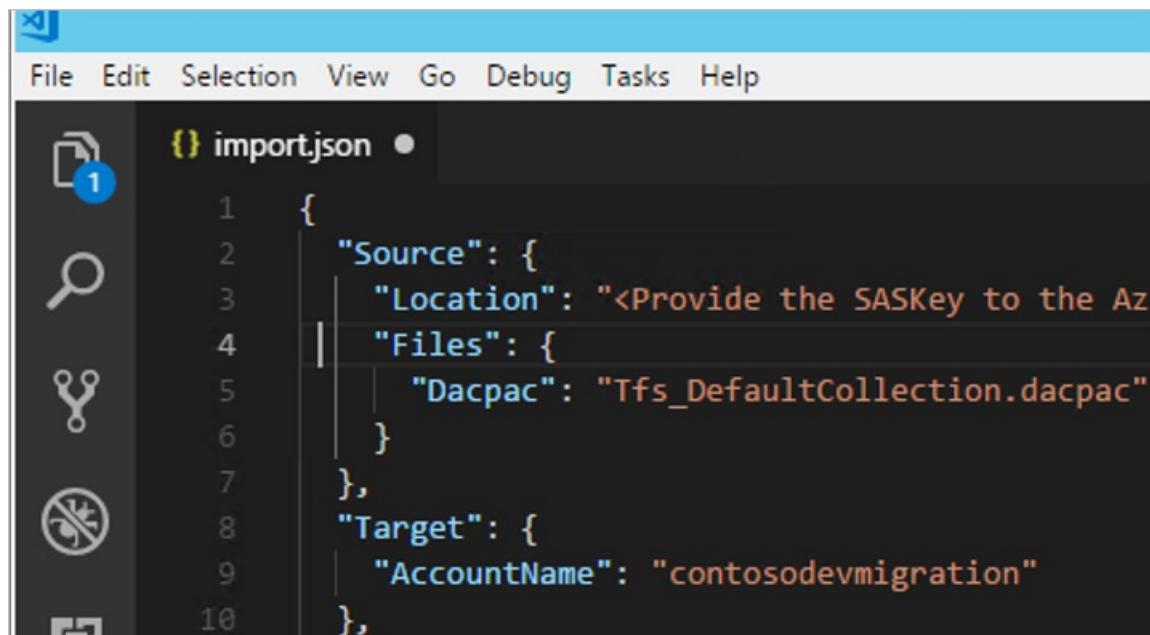
3. The preparation is completed, and the tool reports that the import files have been generated successfully.

```
-----  
Generating Import Files  
-----  
  
Collection validation successful.  
Generating required import files...  
  
Prepare WorkItem Tracking Data Import      Passed  
Prepare Import Package                    Passed  
  
-----  
Guidance  
-----  
  
Now that the files are generated, recommended next steps are:  
  
1) Review each generated file and make changes or fill in blanks as needed  
2) See TfsMigrator validate /help for instructions on re-validating the files  
3) Once satisfied you'll need to ready the collection for import
```

4. The admins can now see that both the `IdentityMapLog.csv` file and the `import.json` file have been created in a new folder.

Name	Date modified	Type	Size
Logs	6/12/2018 12:27 PM	File folder	
Collection	6/12/2018 12:27 PM	Text Document	14 KB
IdentityMapLog	6/12/2018 12:27 PM	Microsoft Excel C...	2 KB
import	6/12/2018 12:27 PM	JSON File	2 KB
PrepareDataImportPackage	6/12/2018 12:27 PM	Text Document	3 KB
ProcessMapImportPreparator	6/12/2018 12:27 PM	Text Document	1 KB
ProjectProcessesMap	6/12/2018 12:27 PM	Text Document	6 KB
TfsMigrator	6/12/2018 12:27 PM	Text Document	33 KB

5. The `import.json` file provides import settings. It includes information such as the desired organization name, and storage account details. Most of the fields are populated automatically. Some fields require user input. The admins open the file and add the Azure DevOps Services organization name to be created, `contosodevmigration`. With this name, the Contoso Azure DevOps Services URL will be `contosodevmigration.visualstudio.com`.



```

1  {
2    "Source": {
3      "Location": "<Provide the SASKey to the Azu",
4      "Files": {
5        "Dacpac": "Tfs_DefaultCollection.dacpac"
6      }
7    },
8    "Target": {
9      "AccountName": "contosodevmigration"
10 },

```

#### NOTE

The organization must be created before the migration begins. It can be changed after the migration is completed.

6. The admins review the identity log map file, which shows the accounts that will be brought into Azure DevOps Services during the import.
- Active identities refer to identities that will become users in Azure DevOps Services after the import.
  - In Azure DevOps Services, these identities will be licensed and displayed as users in the organization after migration.
  - The identities are marked as **Active** in the **Expected Import Status** column in the file.

A	B	C	D
1 AD: User(TFS)	AAD: Security Identifier	AAD: Expected Import User(VSTS)	Expected Import Status
2 CONTOSOTFS\Administrator	S-1-5-21-13773882-1227584077-4008836372-500	No Match Found (Check AAD Sync)	Historical
3 CONTOSO\Administrator	S-1-5-21-922643139-2624149876-687917293-500	No Match Found (Check AAD Sync)	Historical
4 CONTOSO\antf	S-1-5-21-922643139-2624149876-687917293-3946	antf@contosomigration.onmicrosoft.com	Active
5 CONTOSO\dand	S-1-5-21-922643139-2624149876-687917293-3945	dand@contosomigration.onmicrosoft.com	Active
6 CONTOSO\Frec	S-1-5-21-922643139-2624149876-687917293-3949	Frec@contosomigration.onmicrosoft.com	Active
7 CONTOSO\Kart	S-1-5-21-922643139-2624149876-687917293-3948	Kart@contosomigration.onmicrosoft.com	Active
8 CONTOSO\Mara	S-1-5-21-922643139-2624149876-687917293-3957	Mara@contosomigration.onmicrosoft.com	Active
9 CONTOSO\Rhoh	S-1-5-21-922643139-2624149876-687917293-3963	Rhoh@contosomigration.onmicrosoft.com	Active

## Step 5: Migrate to Azure DevOps Services

With the preparation completed, Contoso admins can focus on the migration. After they run the migration, they'll switch from using TFVC to Git for version control.

Before they start, the admins schedule downtime with the dev team, so that they can plan to take the collection offline for migration.

Here is the migration process they'll follow:

1. **Detach the collection.** Identity data for the collection resides in the configuration database for the Team Foundation Server instance while the collection is attached and online.

When a collection is detached from the Team Foundation Server instance, a copy of that identity data is made and then packaged with the collection for transport. Without this data, the identity portion of the import can't be executed.

We recommended that the collection stay detached until the import has been completed, because changes that occur during the import can't be imported.

2. **Generate a backup.** The next step is to generate a backup that can be imported into Azure DevOps Services. The data-tier application component package (DACPAC) is a SQL Server feature that allows database changes to be packaged into a single file and then deployed to other instances of SQL.

The backup can also be restored directly to Azure DevOps Services, and it's used as the packaging method for getting collection data to the cloud. Contoso will use the `sqlpackage.exe` tool to generate the DACPAC. This tool is included in SQL Server Data Tools.

3. **Upload to storage.** After the DACPAC is created, the admins upload it to Azure Storage. After they've uploaded it, they get a shared access signature (SAS) to allow the Team Foundation Server migration tool access to the storage.
4. **Fill out the import.** Contoso can then complete the missing fields in the import file, including the DACPAC setting. To ensure that everything's working properly before the full migration, the admins will specify that they want to perform a *dry-run* import.
5. **Perform a dry-run import.** A dry-run import helps them test the collection migration. Dry runs have a limited life, so they're deleted before a production migration runs. They're deleted automatically after a set duration. A note that informs Contoso when the dry run will be deleted is included in the success email that's sent after the import finishes. The team takes note and plans accordingly.
6. **Complete the production migration.** With the dry-run migration completed, Contoso admins do the final migration by updating the `import.json` file and then running import again.

### Detach the collection

Before they detach the collection, Contoso admins take a local SQL Server instance backup and a VMware snapshot of the Team Foundation Server instance.

1. In the Team Foundation Server Administration Console, the admins select the collection they want to detach, `ContosoDev`.

The screenshot shows the 'Team Project Collections' section of the TFS Administration Console. On the left, a navigation tree shows 'CONTOSOTFS' > 'Application Tier' > 'Team Project Collections'. The main pane lists two collections:

Name	State
ContosoDev	Online
DefaultCollection	Online

- They select the General tab and then select Detach Collection.

The screenshot shows the 'General' tab for the 'ContosoDev' collection. It displays the URL (http://contosotfs:8080/tfs/ContosoDev/) and the SQL Server Instance (CONTOSOTFS\SqlExpress). On the right, there are several actions: Stop Collection, Edit Settings, Group Membership, Administer Security, and Detach Collection, with the 'Detach Collection' button highlighted by a red box.

- In the Detach Team Project Collection wizard, on the Servicing Message pane, the admins provide a message for users who might try to connect to projects in the collection.

The screenshot shows the 'Servicing Message' pane of the 'Detach Team Project Collection' wizard. It provides instructions for disconnecting the collection from the TFS server. A message box contains the text: 'This Collection is being migrated to VSTS. Please see your administrator for more details.'

- On the Detach Progress pane, they monitor progress. When the process finishes, they select Next.

 Detach Team Project Collection

Servicing Message  
Review Configuration  
Readiness Checks

**Detach Progress**

Complete

Monitor the Team Project Collection detach progress.  
The Team Project Collection detach has completed.

 Succeeded

Steps Completed: 30 of 30  
Elapsed Time: 00:10  
Issues: None

[Click here to view the log](#)

Team Foundation Server 2018 Update 2      Previous      **Next**      Complete      Close

5. On the **Readiness Checks** pane, when the checks finish, they select **Detach**.

 Detach Team Project Collection

Servicing Message  
Review Configuration  
**Readiness Checks**

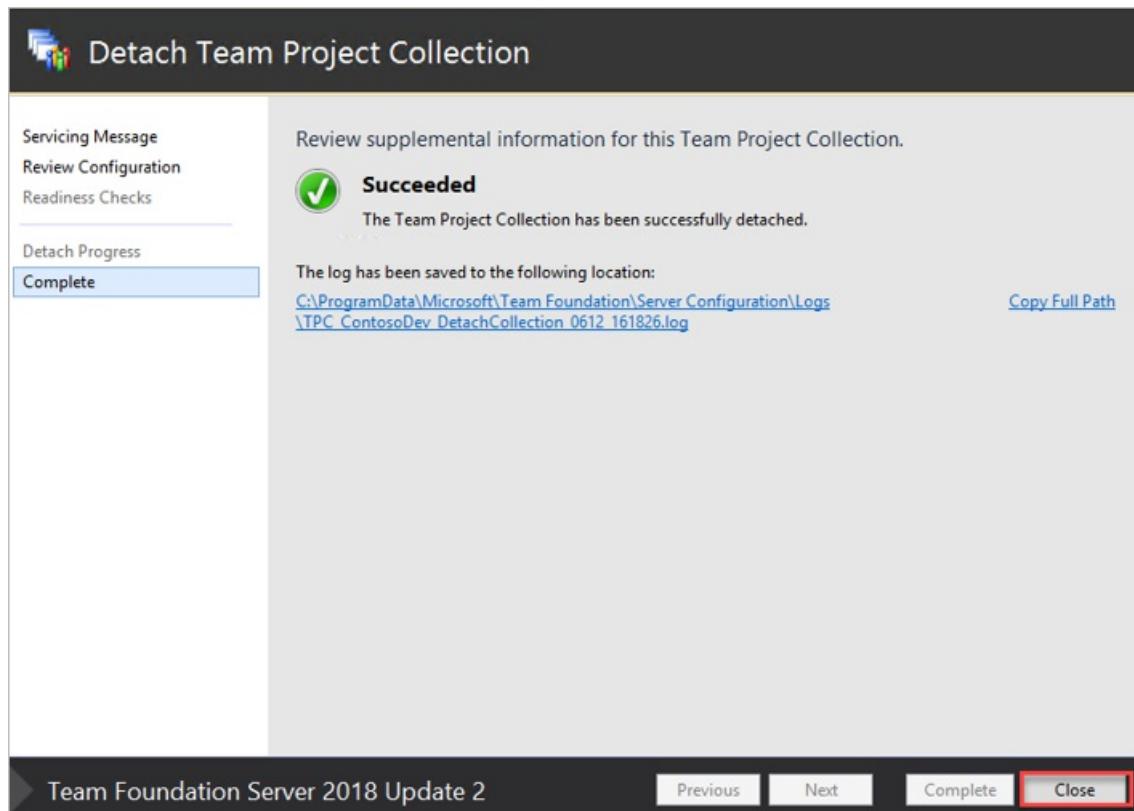
Detach Progress  
Complete

Readiness checks verify that your Team Project Collection is ready to be detached.  
Readiness checks passed.

 Collection servicing status      Passed

Team Foundation Server 2018 Update 2      Previous      Next      **Detach**      Cancel

6. When the collection has been successfully detached, they select **Close** to finish up.



The collection is no longer referenced in the Team Foundation Server Administration Console.

Name	State
DefaultCollection	Online

### Generate a DACPAC

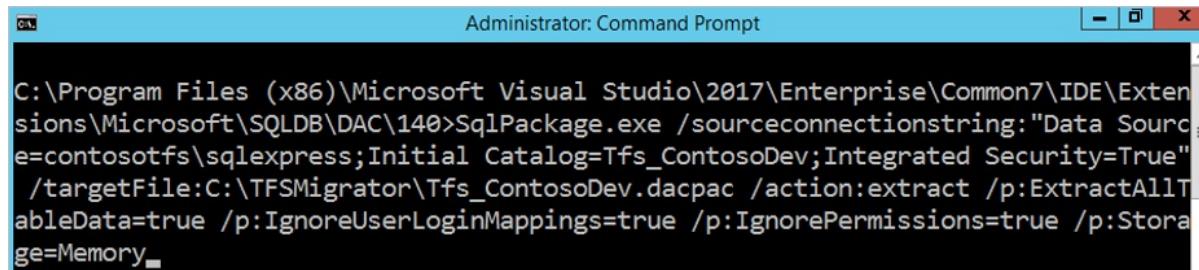
Contoso admins create a backup, or DACPAC, to import into Azure DevOps Services.

- The admins use the `sqlpackage.exe` utility in SQL Server Data Tools (SSDT) to create the DACPAC. There are multiple versions of `sqlpackage.exe` installed with SQL Server Data Tools, and they're located under folders with names like `120`, `130`, and `140`. It's important to use the right version to prepare the DACPAC.
- Team Foundation Server 2018 imports need to use `sqlpackage.exe` from the `140` folder or higher. For `CONTOSOTFS`, this file is located in  
`C:\Program Files (x86)\Microsoft Visual Studio\2017\Enterprise\Common7\IDE\Extensions\Microsoft\SQLDB\DAC\140`

Contoso admins generate the DACPAC as follows:

- They open a command prompt and go to the `sqlpackage.exe` location. To generate the DACPAC, they run the following command:

```
SqlPackage.exe /sourceconnectionstring:"Data Source=SQLSERVERNAME\INSTANCENAME;Initial Catalog=Tfs_ContosoDev;Integrated Security=True" /targetFile:C:\TFSMigrator\Tfs_ContosoDev.dacpac /action:extract /p:ExtractAllTableData=true /p:IgnoreUserLoginMappings=true /p:IgnorePermissions=true /p:Storage=Memory
```

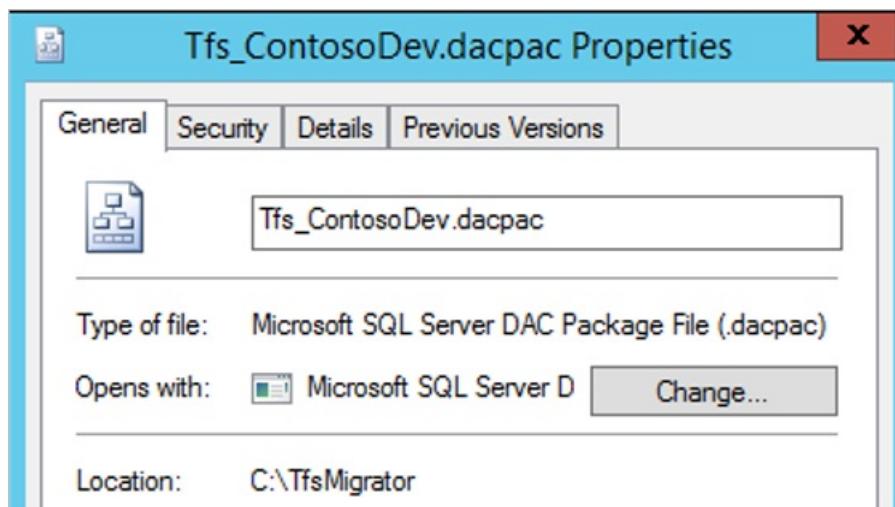


```
Administrator: Command Prompt
C:\Program Files (x86)\Microsoft Visual Studio\2017\Enterprise\Common7\IDE\Extensions\Microsoft\SQLDB\DAC\140>SqlPackage.exe /sourceconnectionstring:"Data Source=contosotfs\sqlexpress;Initial Catalog=Tfs_ContosoDev;Integrated Security=True" /targetFile:C:\TFSMigrator\Tfs_ContosoDev.dacpac /action:extract /p:ExtractAllTableData=true /p:IgnoreUserLoginMappings=true /p:IgnorePermissions=true /p:Storage=Memory
```

The following message is displayed:

```
Processing Table '[dbo].[tbl_OrchestrationSession]'.
Processing Table '[dbo].[tbl_TestResultInsights]'.
Successfully extracted database and saved it to file 'C:\TFSMigrator\Tfs_ContosoDev.dacpac'.
```

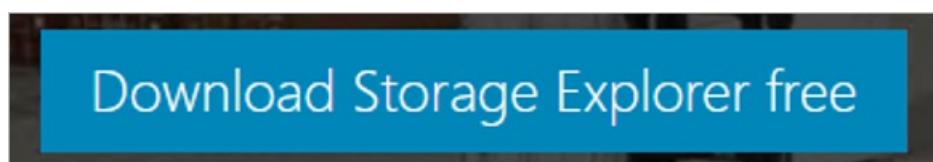
2. They verify the properties of the DACPAC file.



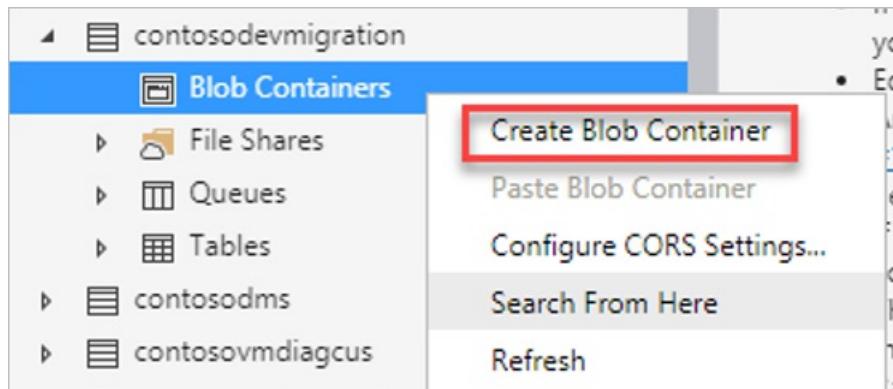
### Upload the file to storage

After the admins create the DACPAC file, they upload it to the Azure storage account.

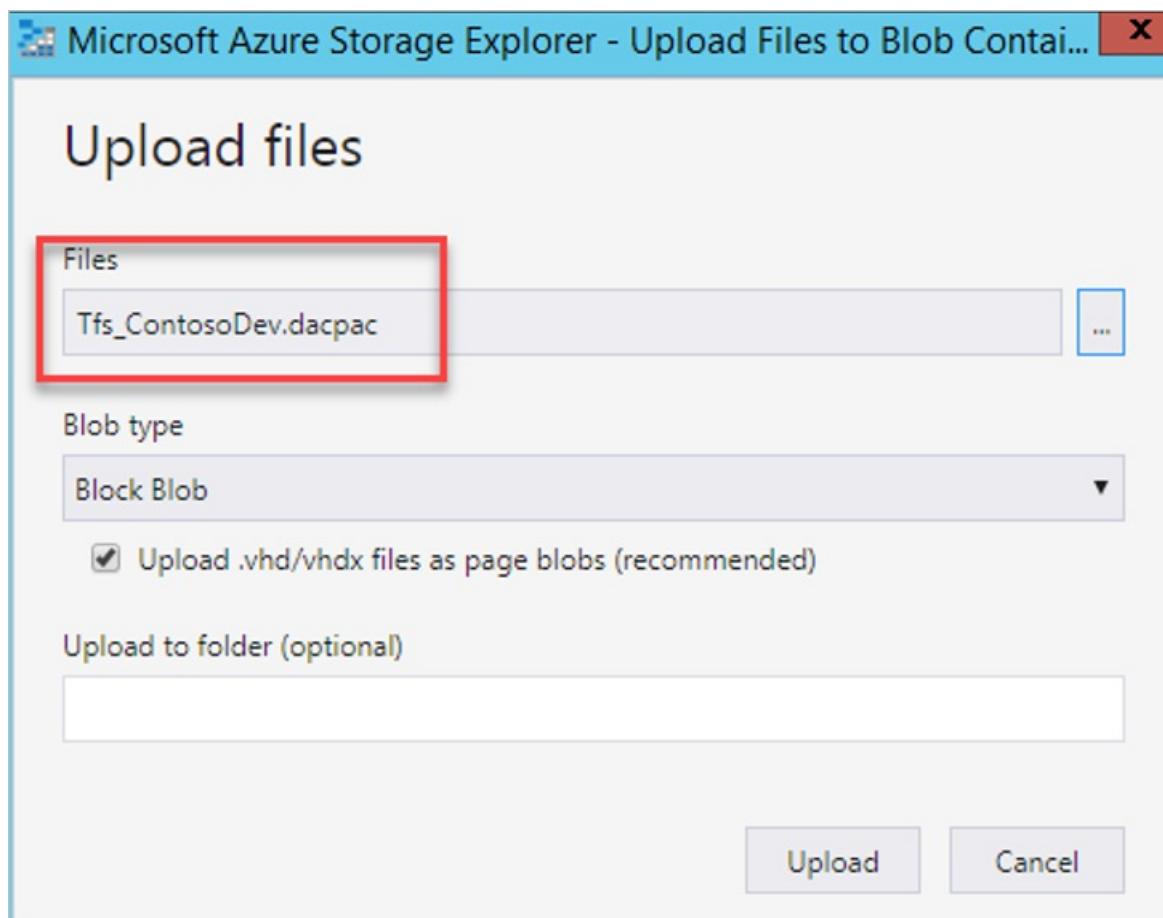
1. They download and install [Azure Storage Explorer](#).



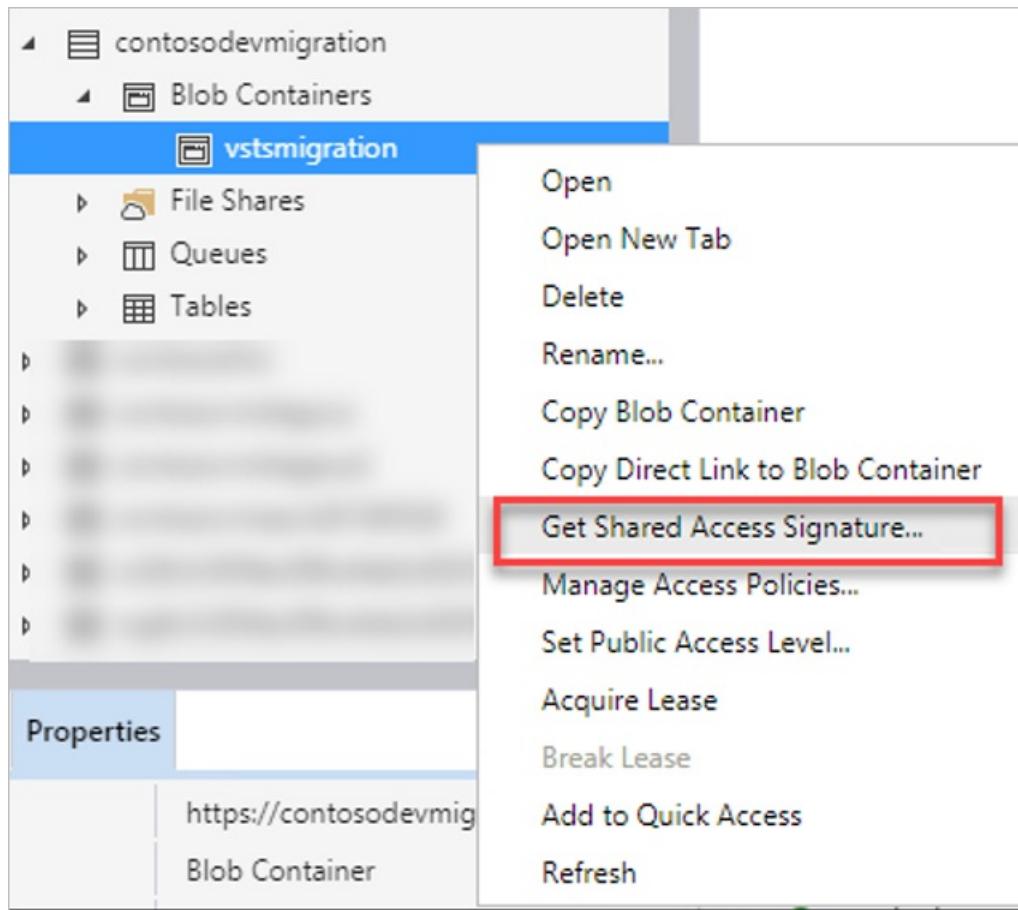
2. In Storage Explorer, the admins connect to their subscription and then search for and select the storage account they created for the migration (`contosodevmigration`). They create a new blob container, `azuredevopsmigration`.



3. On the Upload files pane, in the Blob type drop-down list, the admins specify Block Blob for the DACPAC file upload.



4. After they upload the file, they select the file name and then select Generate SAS. They expand the Blob Containers list under the storage account, select the container with the import files, and then select Get Shared Access Signature.



5. On the **Shared Access Signature** pane, they accept the default settings and then select **Create**. This enables access for 24 hours.

## Shared Access Signature

Access policy:

(none)

Start time:

06/12/2018 05:43 PM

Expiry time:

06/13/2018 05:43 PM

Time zone:

- Local  
 UTC

Permissions:

- Read  
 Write  
 Delete  
 List

- They copy the shared access signature URL, so that it can be used by the Team Foundation Server migration tool.

## Shared Access Signature

Container:

vstsmigration

URL:

<https://contosodevmigration.blob.core.windows.net/vstsmigration>

Copy

Query string:

?st=2018-06-12T21%3A43%3A17Z&se=2018-06-13T21%3A43%

Copy

### NOTE

The migration must happen within the allowed time window or the permissions will expire. Do *not* generate an SAS key from the Azure portal. Keys that are generated from the portal are account-scoped and won't work with the import.

### Fill in the import settings

Earlier, Contoso admins partially filled in the import specification file, *import.json*. Now, they need to add the remaining settings.

They open the *import.json* file and complete the following fields:

- **Location:** They enter the location of the SAS key that was generated previously.
- **Dacpac:** They enter the name of the DACPAC file that they uploaded earlier to the storage account, making sure to include the *.dacpac* extension.
- **ImportType:** They enter **DryRun** for now.

```
{
  "Source": {
    "Location": "https://contosodevmigration.blob.core.windows.net/vstsmigration?st=2018-06-12T21%3A43%3A17Z&se=2018-06-13T21%3A43%",
    "Files": {
      "Dacpac": "Tfs_ContosoDev.dacpac"
    }
  },
  "Target": {
    "AccountName": "contosodevmigration"
  },
  "Properties": {
    "ImportType": "DryRun"
  }
}
```

### Perform a dry-run migration

Contoso admins perform a dry-run migration to make sure that everything's working as expected.

1. They open a command prompt and then go to the `TfsMigrator` location (`C:\TFSMigrator`).
2. They want to make sure that the file is formatted properly and that the SAS key is working. They validate the import file by running the following command:

```
TfsMigrator import /importFile:C:\TFSMigrator\import.json /validateonly
```

The validation returns an error saying that the SAS key needs a longer period before it expires.

Administrator: Command Prompt

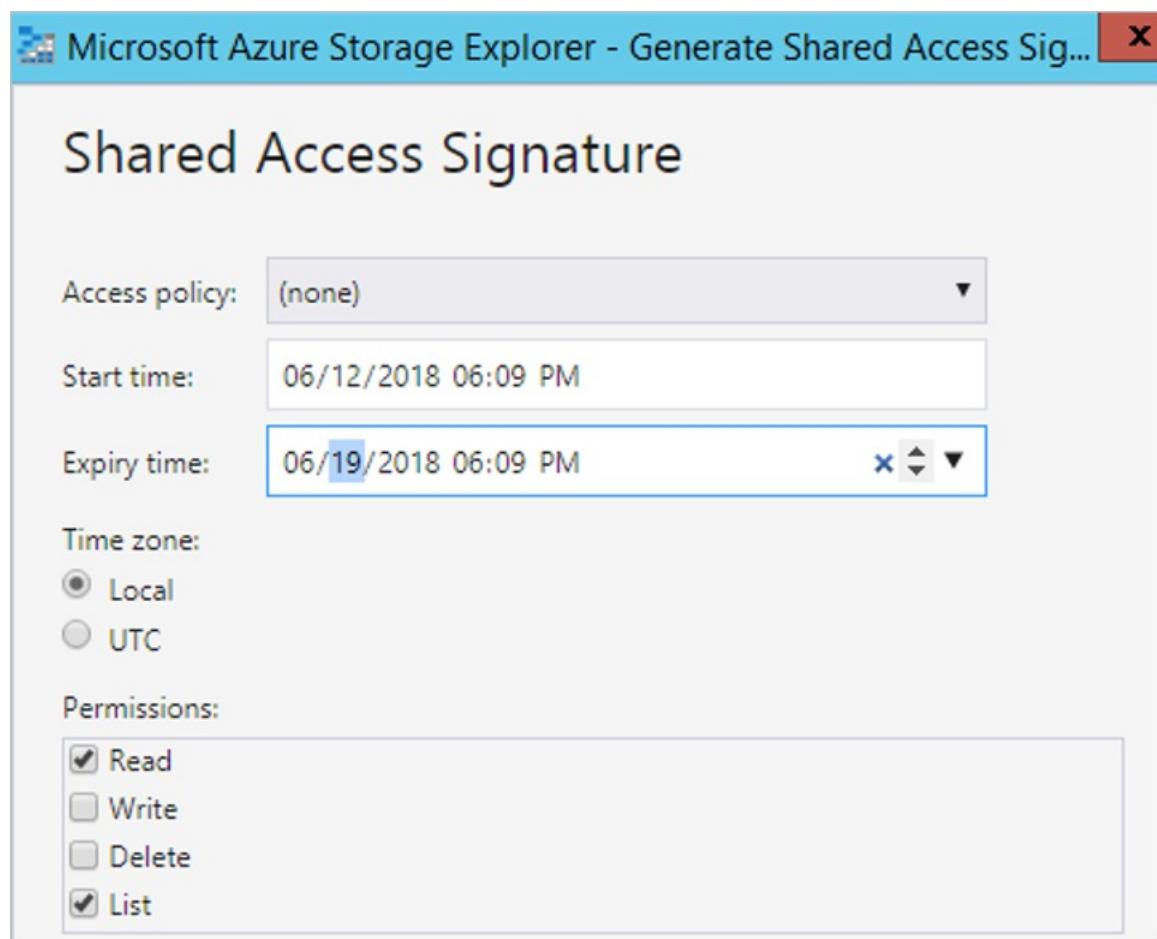
```
C:\TFSMigrator>TfsMigrator import /importFile:C:\TFSMigrator\import.json /validateonly
Microsoft Team Foundation Server (R) Tfs Migrator Tool version 16.131.27716.2
Copyright (C) Microsoft Corporation. All rights reserved.

-----
Validating Import File
-----

Validating import specification file...

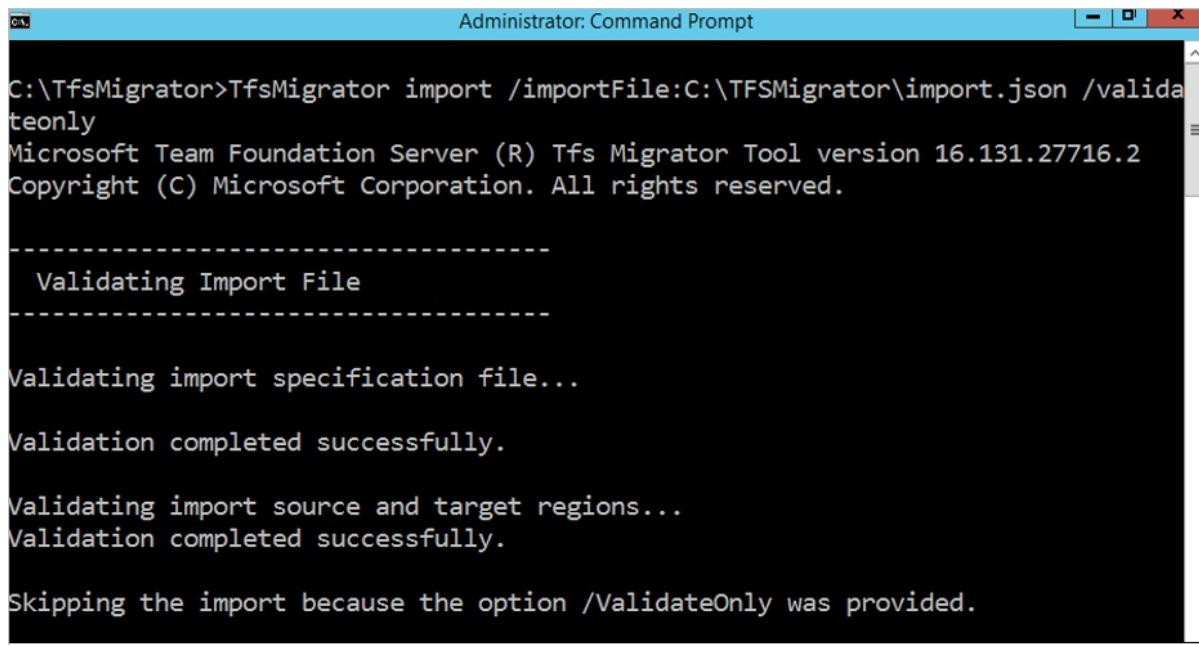
Validation completed with an error.
+ [Error] VS403381: The provided SAS key's expiration time is not sufficient to
perform the import. The key will expire in 0.97 days, but the import requires at
least 3 days of validity remaining to perform the import. See the instructions
on the following page to generate a new SAS key: https://aka.ms/GenerateSASKey
```

3. They use Azure Storage Explorer to create a new SAS key with the period before expiration set to seven days.



4. They update the `import.json` file and rerun the command. This time, the validation is completed successfully.

```
TfsMigrator import /importFile:C:\TFSMigrator\import.json /validateonly
```



Administrator: Command Prompt

```
C:\TfsMigrator>TfsMigrator import /importFile:C:\TFSMigrator\import.json /validateonly
Microsoft Team Foundation Server (R) Tfs Migrator Tool version 16.131.27716.2
Copyright (C) Microsoft Corporation. All rights reserved.

-----
Validating Import File
-----

Validating import specification file...
Validation completed successfully.

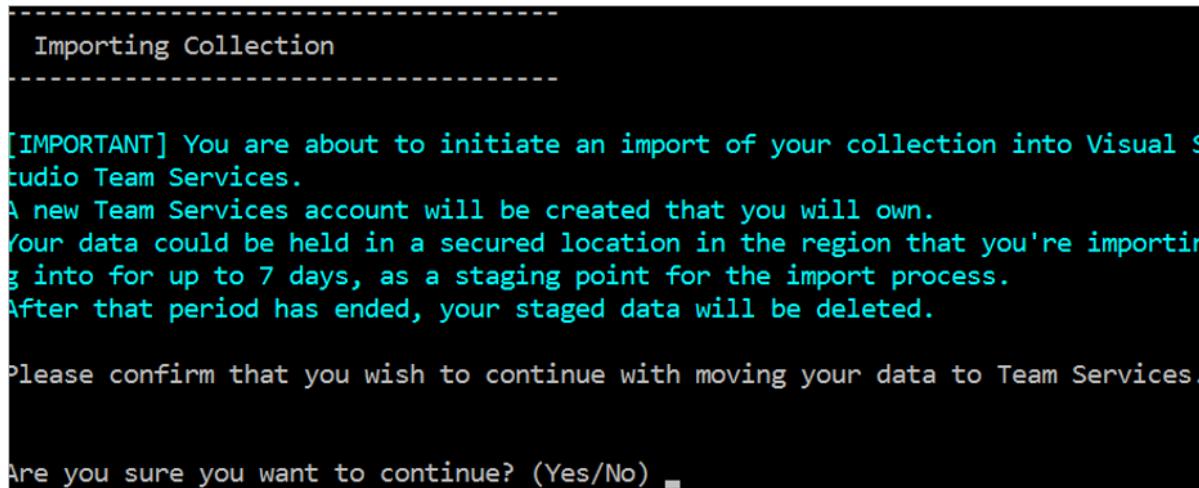
Validating import source and target regions...
Validation completed successfully.

Skipping the import because the option /ValidateOnly was provided.
```

5. They start the dry run by running the following command:

```
TfsMigrator import /importFile:C:\TFSMigrator\import.json
```

A message is displayed asking them to confirm that they want to continue with the migration. Note the seven-day period after the dry run during which the staged data will be maintained.



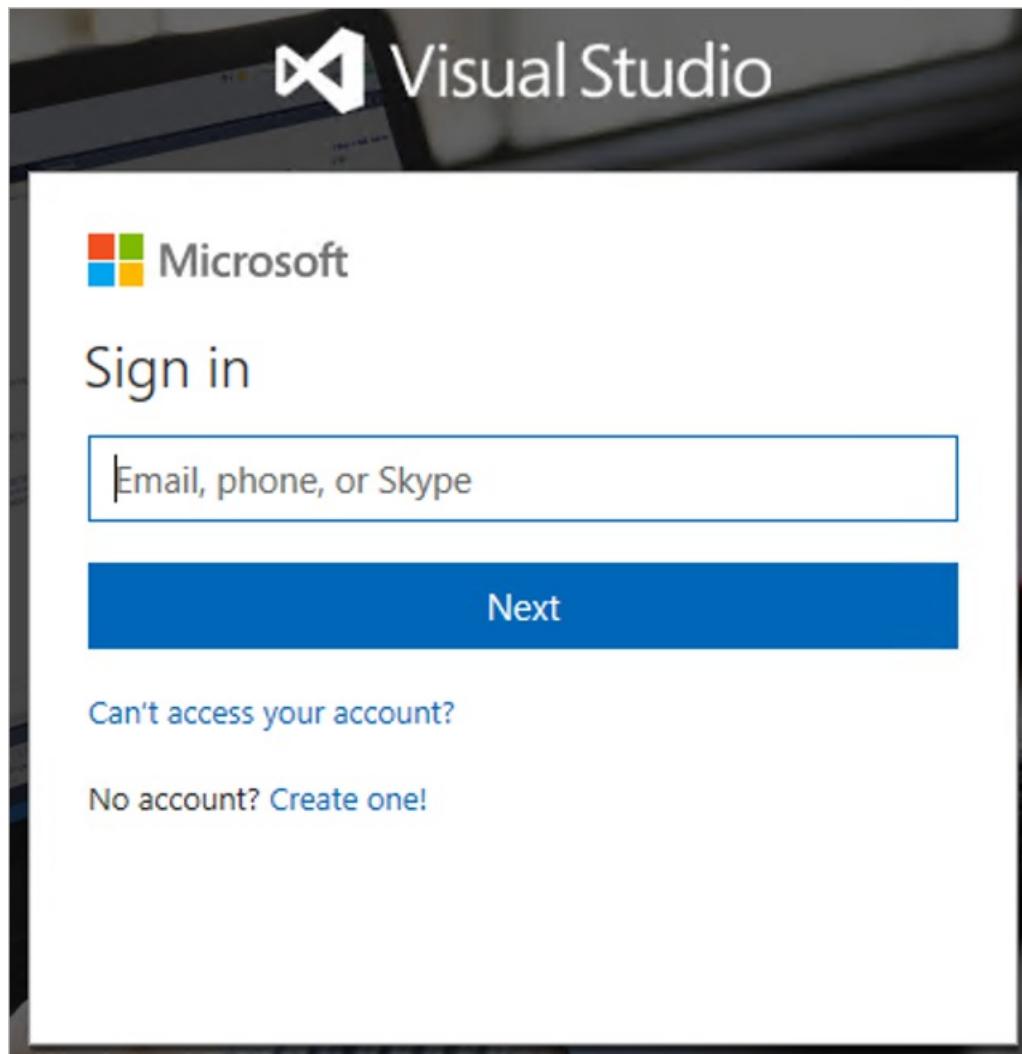
```
-----
Importing Collection
-----

[IMPORTANT] You are about to initiate an import of your collection into Visual Studio Team Services.
A new Team Services account will be created that you will own.
Your data could be held in a secured location in the region that you're importing into for up to 7 days, as a staging point for the import process.
After that period has ended, your staged data will be deleted.

Please confirm that you wish to continue with moving your data to Team Services.

Are you sure you want to continue? (Yes/No)
```

6. The Azure AD sign-in window opens. Contoso admins sign in to Azure AD with admin permissions.



A message is displayed confirming that the import has been started successfully.

```
Starting the Import ...
Import has been successfully started!
Monitor import: https://contosodevmigration-dryrun.visualstudio.com
Import ID: b954df07-4965-42c6-8439-
```

7. After about 15 minutes, the admins go to the website and see the following information:



## Importing to **Contosodevmigration-Dryrun**



### Restoring your collection (Step 1 of 7)

First, we need to ensure that your collection is restored into a database. That way we can pull your data into Visual Studio Team Services. This step might take a while, but we promise we're still making progress on your import!

8. After the migration finishes, a Contoso dev lead signs in to Azure DevOps Services to ensure that the dry run worked properly. After authentication, Azure DevOps Services needs a few details to confirm the organization.

# We need a few more details

Your name:

Anthony Frizzell

We'll reach you at:

antf@contosomigration.onmicrosoft.com

From:

United States ▾

Microsoft may use your contact information to provide updates and special offers about Visual Studio. You can unsubscribe at any time.

Continue

The dev lead can see that the projects have been migrated successfully. A notice near the top of the page warns that the dry run account will be deleted in 15 days.

The screenshot shows the Microsoft Dev Center interface. At the top, it says "Good evening, Anthony Frizzell". Below that, there is a red box highlighting a warning message: "VS403262: This dry run account will expire and be deleted shortly after or on 6/27/2018. To continue testing beyond this date you will need to repeat the dry run import." The main area shows a list of projects: "PolicyConnect" and "SmartHotelContainer". There is also a "New Project" button.

9. The dev lead opens one of the projects and then selects **Work Items > Assigned to me**. This page verifies that the work item data has been migrated successfully, along with the identity.

Work Items					
Assigned to me		+ New Work Item	Open in Queries	Column Options	Recycle Bin
Filter by keyword		Types	States	Area	
ID	Title		State	Area Path	
74	Q2 - Feature 6 - PBI - 8	...	Approved	PolicyConnect	
43	2018 - Q2 - Initiatives	...	In Progress	PolicyConnect	
77	2018 - Q3 - Initiatives	...	New	PolicyConnect	
142	Q3 - Feature 12 - PBI - 8	...	New	PolicyConnect	
131	Q3 - Feature 11 - PBI - 8	...	New	PolicyConnect	
120	Q3 - Feature 10 - PBI - 8	...	New	PolicyConnect	
111	2018 - Q4 - Initiatives	...	New	PolicyConnect	
108	Q3 - Feature 9 - PBI - 8	...	New	PolicyConnect	
97	Q3 - Feature 8 - PBI - 8	...	New	PolicyConnect	
86	Q3 - Feature 7 - PBI - 8	...	New	PolicyConnect	

10. To confirm that the source code and history have been migrated, the dev lead checks other projects and code.

The screenshot shows the 'History' tab for the '\$/SmartHotelContainer' folder. It displays two changesets:

- Updated Dockerfile - remove default site**: Administrator created on Sunday, June 10, 2018. This change includes a file named 'Dockerfile'.
- Deleted wwwroot**: Administrator created on Sunday, June 10, 2018. This change includes a folder named 'wwwroot'.

### Run the production migration

Now that the dry run is complete, Contoso admins move on to the production migration. They delete the dry-run organization, update the import settings, and run import again.

1. In the Azure DevOps Services portal, they delete the dry-run organization.
2. They update the `import.json` file to set the `ImportType` to `ProductionRun`.

## { } import.json ●

```
1
2 "Source": {
3     "Location": "https://contosodevmigration.blob.
4     "Files": {
5         "Dacpac": "Tfs_ContosoDev.dacpac"
6     }
7 },
8 "Target": {
9     "AccountName": "contosodevmigration"
10 },
11 "Properties": {
12     "ImportType": "ProductionRun"
```

3. As they did for the dry run, they start the migration by running the following command:

```
TfsMigrator import /importFile:C:\TFSMigrator\import.json .
```

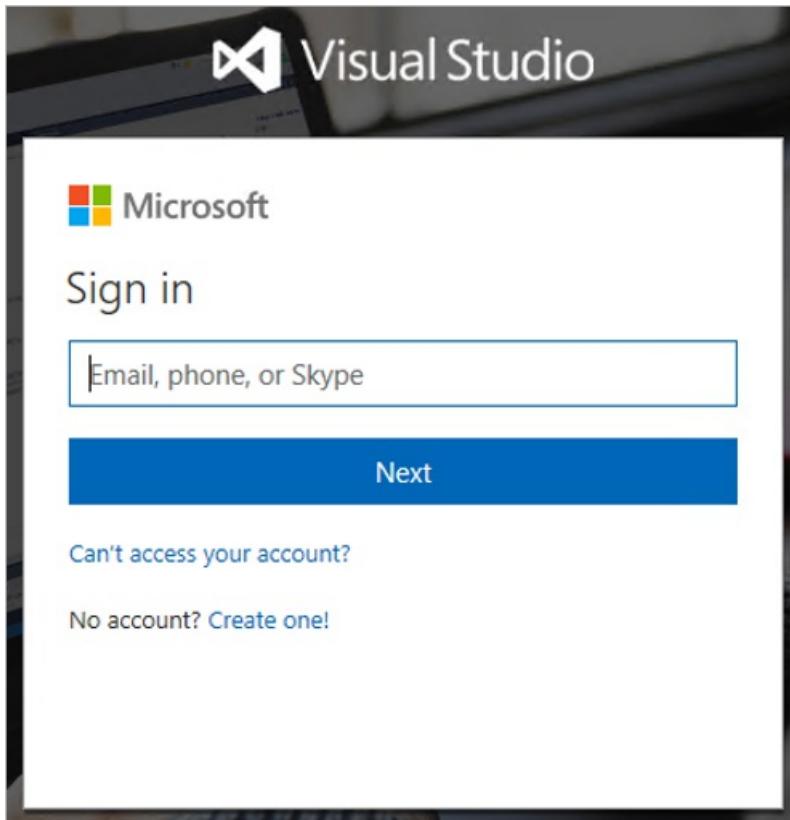
A message is displayed asking the admins to confirm the migration. It warns that data could be held in a secure location as a staging area for up to seven days.

```
Importing Collection
-----
[IMPORTANT] You are about to initiate an import of your collection into Visual Studio Team Services.
A new Team Services account will be created that you will own.
Your data could be held in a secured location in the region that you're importing into for up to 7 days, as a staging point for the import process.
After that period has ended, your staged data will be deleted.

Please confirm that you wish to continue with moving your data to Team Services

Are you sure you want to continue? (Yes/No) yes_
```

4. In the Azure AD sign-in window, they specify a Contoso admin sign-in.



A message is displayed that the import has started successfully.

```
Starting the Import ...
Import has been successfully started!
Monitor import: https://contosodevmigration.visualstudio.com
Import ID: 715a1aa1-82f0-45ca-843d-a0a0e8720388
```

- After about 15 minutes, the admins go to the website and see the following information:



## Importing to **Contosodevmigration**



### Copying your data to the cloud (Step 3 of 7)

We're busy moving your data to the cloud. This is the longest step **in the process** and it could take several hours. We promise we're still making progress on your import!

- After the migration finishes, a dev lead signs into Azure DevOps Services to ensure that the migration worked properly. After signing in, the dev lead can see that projects have been migrated.

The screenshot shows the Azure DevOps Services interface. At the top, there's a navigation bar with links for 'Projects', 'My favorites', 'My work items', 'My pull requests', and more. The main area is titled 'contosodevmigration' and displays a message 'Good evening, Anthony Frizzell'. Below this, there's a section for 'Projects' with a 'Filter projects and' input field. Under 'All' projects, two are listed: 'PolicyConnect' and 'SmartHotelContainer', each represented by a small icon and a link.

- The dev lead opens one of the projects and selects **Work Items > Assigned to me**. This shows that the work item data has been migrated, along with the identity.

Work Items				
Assigned to me		+ New Work Item	Open in Queries	Column Options
Filter by keyword		Types	States	Area
ID	Title		State	Area Path
74	Q2 - Feature 6 - PBI - 8	...	Approved	PolicyConnect
43	2018 - Q2 - Initiatives	...	In Progress	PolicyConnect
77	2018 - Q3 - Initiatives	...	New	PolicyConnect
142	Q3 - Feature 12 - PBI - 8	...	New	PolicyConnect
131	Q3 - Feature 11 - PBI - 8	...	New	PolicyConnect
120	Q3 - Feature 10 - PBI - 8	...	New	PolicyConnect
111	2018 - Q4 - Initiatives	...	New	PolicyConnect
108	Q3 - Feature 9 - PBI - 8	...	New	PolicyConnect
97	Q3 - Feature 8 - PBI - 8	...	New	PolicyConnect
86	Q3 - Feature 7 - PBI - 8	...	New	PolicyConnect

8. The dev lead checks to confirm that other work item data has been migrated.

Order	Work Item Type	Title	State	Effort	Assigned To
1	Epic	2018 - Q2 - Initiatives	In Progress		Anthony Frizzell
	Feature	Q2 - Feature 4	Done		Dan Drayton
	Product Backlog Item	Q2 - Feature 4 - PBI - 1	Done		Freda Conley
	Product Backlog Item	Q2 - Feature 4 - PBI - 2	Done		Freda Conley
	Product Backlog Item	Q2 - Feature 4 - PBI - 3	Done		Margo Ayers
	Product Backlog Item	Q2 - Feature 4 - PBI - 4	Done		Rhonda Hughes
	Product Backlog Item	Q2 - Feature 4 - PBI - 5	Done		Margo Ayers
	Product Backlog Item	Q2 - Feature 4 - PBI - 6	Done		Margo Ayers
	Product Backlog Item	Q2 - Feature 4 - PBI - 7	Done		Dan Drayton
	Product Backlog Item	Q2 - Feature 4 - PBI - 8	Done		Anthony Frizzell
	Product Backlog Item	Q2 - Feature 4 - PBI - 9	Done		Kari Tran
	Product Backlog Item	Q2 - Feature 4 - PBI - 10	Done		Kari Tran
	Feature	Q2 - Feature 5	Done		Dan Drayton
	Feature	Q2 - Feature 6	In Progress		Dan Drayton
2	Epic	2018 - Q3 - Initiatives	New		Anthony Frizzell
3	Epic	2018 - Q4 - Initiatives	New		Anthony Frizzell

9. To confirm that the source code and history have been migrated, the dev lead checks other projects and code.

\$/SmartHotelContainer /

Contents History README

2 changesets

Administrator created #

Sunday, June 10, 2018 2 changesets

Administrator created

Administrator created

### Move source control from TFVC to Git

With the migration now completed, Contoso admins want to move source code management from TFVC to Git. The admins need to import the source code that's currently in their Azure DevOps Services organization as Git repos in the same organization.

1. In the Azure DevOps Services portal, they open one of the TFVC repos, `$/PolicyConnect`, and review it.

\$/PolicyConnect /

Files Changesets Shelvesets

Contents History

Name ↑

ContosolInsurance

ContosolInsurance.sln

2. In the source `$/PolicyConnect` drop-down list, they select **Import repository**.

Screenshot of the PolicyConnect interface showing the 'Files' tab selected. A red box highlights the 'Import repository' option under the 'New repository' section.

3. In the **Source type** drop-down list, they select TFVC. In the **Path** box, they specify the path to the repo, and then select **Import**. They decide to leave the **Migrate History** check box cleared.

Import from TFVC



Source type

TFVC

(i) Migrating from TFVC to Git can be disruptive. Before starting the import, we suggest reading our [documentation](#)

Path \*

\$/PolicyConnect

Migrate History

Name \*

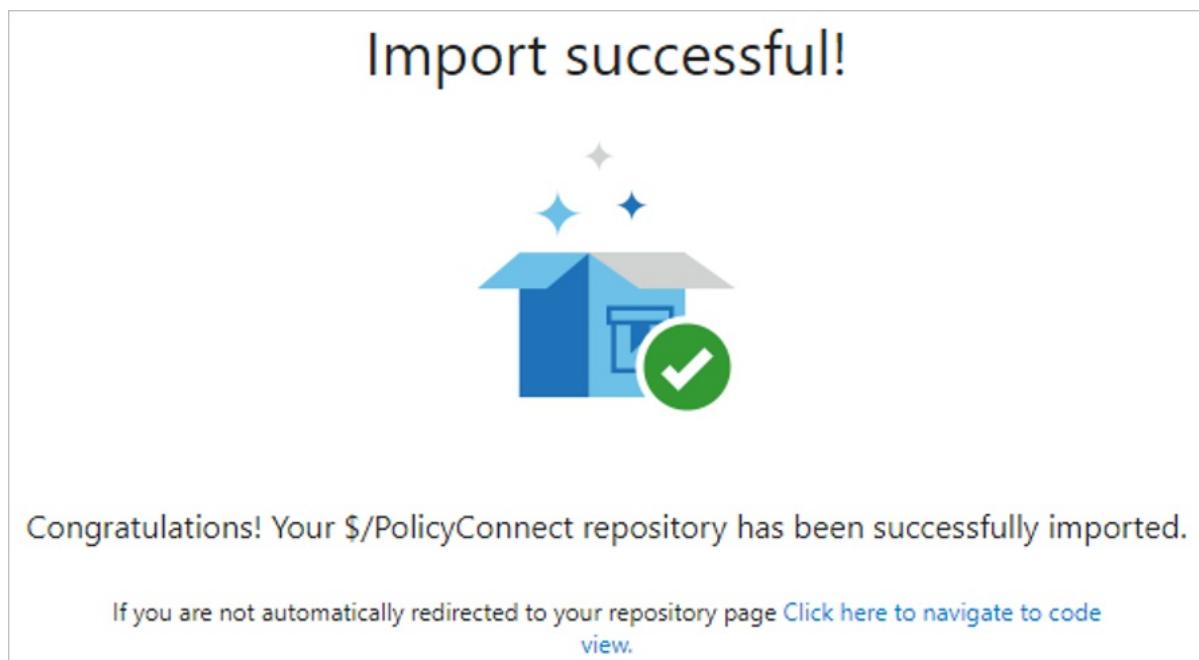
PolicyConnectGit

**Import** **Close**

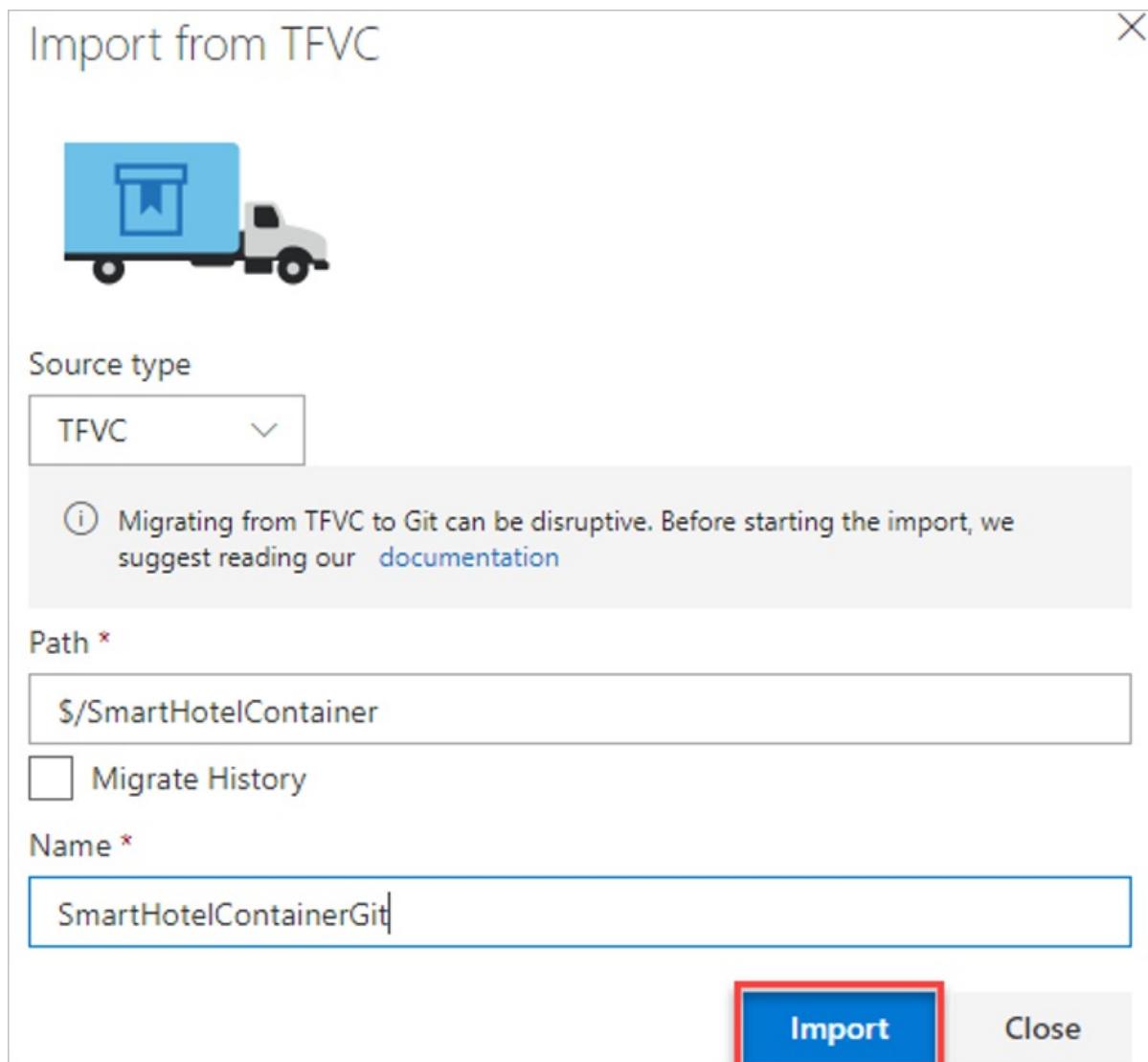
**NOTE**

Because TFVC and Git store version control information differently, we recommend that Contoso *not* migrate its repository history. This is the approach that Microsoft took when we migrated Windows and other products from centralized version control to Git.

4. After the import finishes, the admins review the code.



5. They repeat the process for the second repository, `$/smarthotelcontainer`.



6. After the dev lead reviews the source, they agree that the migration to Azure DevOps Services is done. Azure DevOps Services now becomes the source for all development within the teams involved in the migration.

The screenshot shows a Git repository named "SmartHotelContainerGit" in the "master" branch. The repository contains several files and folders:

Name	Last change
config	11 hours ago
SmartHotelWCF	11 hours ago
SmartHotelWeb	11 hours ago
Dockerfile	11 hours ago
IIS.json	11 hours ago
README.md	11 hours ago

## Need more help?

For more information, see [Import repositories from TFVC to Git](#).

## Clean up after migration

With the migration now complete, the Contoso team needs to do the following:

- Review the [post-import](#) article for information about additional import activities.
- Either delete the TFVC repos or place them in read-only mode. The code bases must not be used, but they can be referenced for their history.

## Post-migration training

The Contoso team will need to provide Azure DevOps Services and Git training for relevant team members.

# Move on-premises VMware infrastructure to Azure

11/9/2020 • 10 minutes to read • [Edit Online](#)

When fictional company Contoso migrates its VMware virtual machines (VMs) from an on-premises datacenter to Azure, two options are available to the team. This article focuses on Azure VMware Solution, which Contoso has determined to be the better migration option.

MIGRATION OPTIONS	OUTCOME
Azure Migrate	<ul style="list-style-type: none"><li>• <a href="#">Assess</a> and <a href="#">migrate</a> on-premises VMs.</li><li>• Run workloads using Azure infrastructure as a service (IaaS).</li><li>• Manage VMs with <a href="#">Azure Resource Manager</a>.</li></ul>
Azure VMware Solution	<ul style="list-style-type: none"><li>• Use VMware Hybrid Cloud Extension (HCX) or vMotion to move on-premises VMs.</li><li>• Run native VMware workloads on Azure bare-metal hardware.</li><li>• Manage VMs using vSphere.</li></ul>

In this article, Contoso uses Azure VMware Solution to create a private cloud in Azure with native access to VMware vCenter and other tools that are supported by VMware for workload migration. Contoso can confidently use Azure VMware Solution, knowing that it's a first-party Microsoft offering backed by VMware.

## Business drivers

Working closely with business partners, the Contoso IT team defines the business drivers for a VMware migration to Azure. These drivers can include:

- **Datacenter evacuation or shutdown:** Seamlessly move VMware-based workloads when they consolidate or retire existing datacenters.
- **Disaster recovery and business continuity:** Use a VMware stack deployed in Azure as a primary or secondary on-demand disaster recovery site for on-premises datacenter infrastructure.
- **Application modernization:** Tap into the Azure ecosystem to modernize Contoso applications without having to rebuild VMware-based environments.
- **Implementing DevOps:** Bring Azure DevOps tool chains to VMware environments and modernize applications at its own pace.
- **Ensure operational continuity:** Redeploy vSphere-based applications to Azure while avoiding hypervisor conversions and application refactoring. Extend support for legacy applications that run Windows and SQL Server.

## Goals for migrating VMware on-premises to VMware in the cloud

With its business drivers in mind, Contoso has pinned down a few goals for this migration:

- Continue managing its existing environments with VMware tools that are familiar to its teams, while modernizing the applications with native Azure services.
- Seamlessly move Contoso VMware-based workloads from its datacenter to Azure, and integrate the VMware environment with Azure.
- After migration, the application in Azure should have the same performance capabilities as it does today in VMware. The application remains as critical in the cloud as it is on-premises.

These goals support Contoso's decision to use Azure VMware Solution and validate it as the best migration method.

## Benefits of running VMware workloads in Azure

By using Azure VMware Solution, Contoso can now seamlessly run, manage, and secure applications across VMware environments and Azure with a common operating framework.

Contoso will capitalize on existing VMware investments, skills, and tools, including VMware vSphere, vSAN, and vCenter. At the same time, Contoso gets the scale, performance, and innovation of Azure. Additionally, it can:

- Set up VMware infrastructure in the cloud in minutes.
- Modernize applications at its own pace.
- Enhance VMware applications with dedicated, isolated, high-performance infrastructure and unique Azure products and services.
- Move or extend on-premises VMs to Azure without having to refactor its applications.
- Get scale, automation, and fast provisioning for VMware workloads on global Azure infrastructure.
- Benefit from a solution that's delivered by Microsoft, verified by VMware, and run on Azure infrastructure.

## The solutions design

After Contoso pins down its goals and requirements, the company designs and reviews a deployment solution and identifies the migration process.

### Current architecture

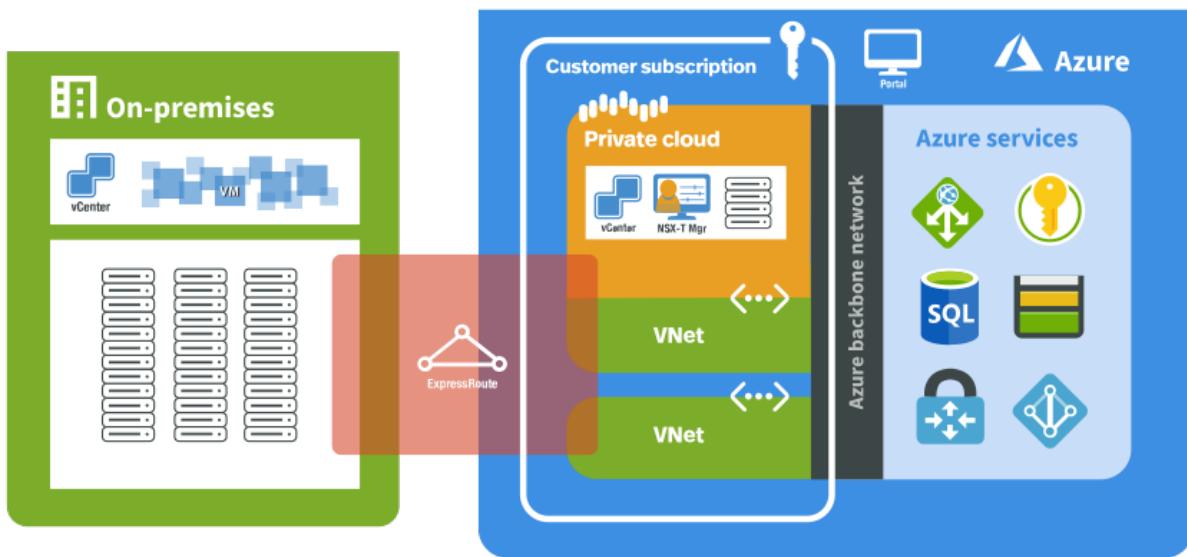
Contoso's current architecture features:

- VMs deployed to an on-premises datacenter that's managed by [vSphere](#).
- Workloads deployed on a VMware ESXi host cluster that's managed with [vCenter](#), [vSAN](#), and [NSX](#).

### Proposed architecture

In its proposed architecture, Contoso will:

- Deploy an [Azure VMware Solution private cloud](#) to the West US Azure region.
- Connect the on-premises datacenter to Azure VMware Solution running in West US by using virtual networks and [ExpressRoute](#) with Global Reach enabled.
- Migrate VMs to dedicated Azure VMware Solution by using [VMware Hybrid Cloud Extension \(HCX\)](#).



## Solution review

Contoso evaluates its proposed design by putting together a pros and cons list, as shown in the following table:

CONSIDERATION	DETAILS
Pros	<ul style="list-style-type: none"> <li>Bare-metal VMware infrastructure with high performance.</li> <li>Infrastructure that's fully dedicated to Contoso and is physically isolated from the infrastructure of other customers.</li> <li>Because Contoso is using a rehost that uses VMware, there's no special configuration or migration complexity.</li> <li>Contoso can take advantage of its investment in Software Assurance by using the <a href="#">Azure Hybrid Benefit</a> and <a href="#">extended security updates</a> for legacy Windows and SQL platforms.</li> <li>Contoso will retain full control of the application VMs in Azure.</li> </ul>
Cons	<ul style="list-style-type: none"> <li>Contoso will need to continue supporting the application as VMware VMs rather than move them to a managed service such as Azure App Service and Azure SQL Database.</li> <li>Azure VMware Solution is set up and priced based on a minimum of three large nodes rather than individual VMs in Azure IaaS. Contoso will need to plan its capacity needs, because the company currently uses an on-premises environment that restricts it from the on-demand nature of other services in Azure.</li> </ul>

### NOTE

For information about pricing, see [Azure VMware Solution pricing](#).

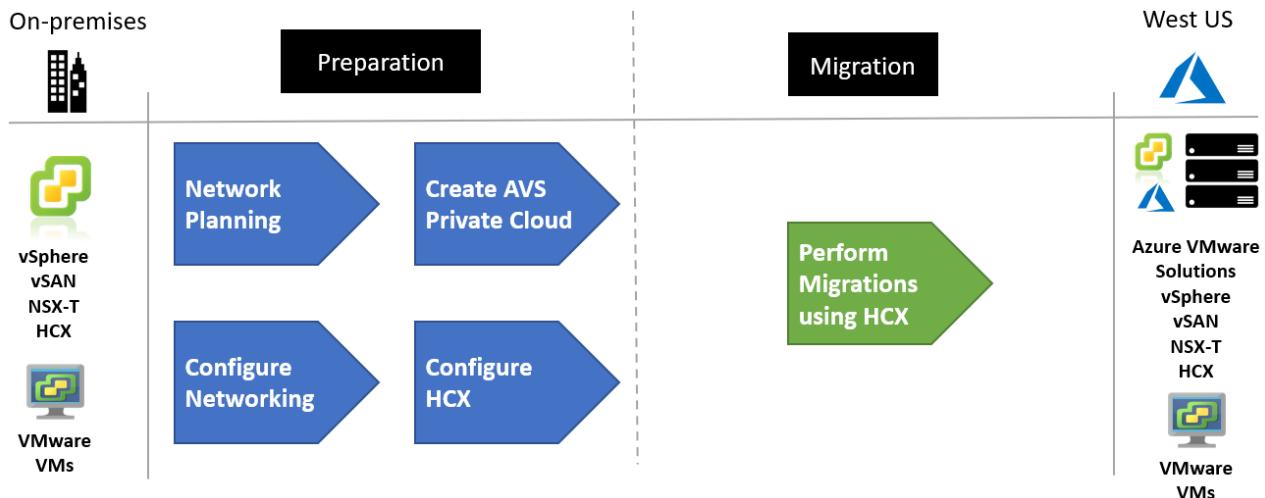
## Migration process

Contoso will move its VMs to Azure VMware Solution by using the VMware HCX tool. The VMs will run in an Azure VMware Solution private cloud. [VMware HCX migration methods](#) include running a bulk or cold migration.

VMware vMotion or Replication-assisted vMotion (RAV) is a method reserved for workloads that run through a live migration.

To complete the process, the Contoso team:

- Plans its networking in Azure and ExpressRoute.
- Creates the Azure VMware Solution private cloud by using the Azure portal.
- Configures the network to include the ExpressRoute circuits.
- Configures the HCX components to connect its on-premises vSphere environment to the Azure VMware Solution private cloud.
- Replicates the VMs and then moves them to Azure by using VMware HCX.



## Scenarios steps

- Step 1: Network planning
- Step 2: Create an Azure VMware Solution private cloud
- Step 3: Configure networking
- Step 4: Migrate VMs using HCX

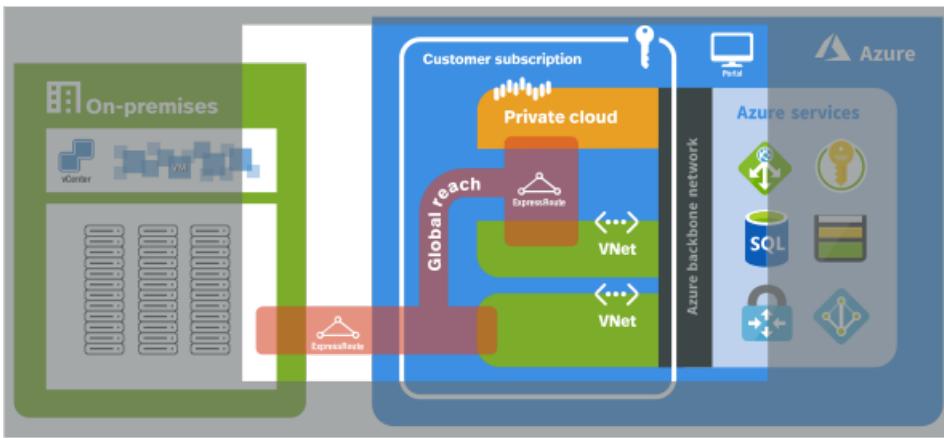
### Step 1: Network planning

Contoso needs to plan out its networking to include Azure Virtual Network and connectivity between on-premises and Azure. The company needs to provide a high-speed connection between its on-premises and Azure-based environments, along with a connection to the Azure VMware Solution private cloud.

This connectivity is delivered through Azure ExpressRoute and will require some specific network address ranges and firewall ports for enabling the services. This high-bandwidth, low-latency connection allows Contoso to access services that run in its Azure subscription from the Azure VMware Solution private cloud environment.

Contoso will need to plan an IP address scheme that includes non-overlapping address space for its [virtual networks](#). The company will need to include a gateway subnet for the [ExpressRoute gateway](#).

The Azure VMware Solution private cloud is connected to Contoso's Azure virtual network by using another Azure ExpressRoute connection. ExpressRoute Global Reach will be enabled to allow [direct connection](#) from on-premises VMs to VMs running on the Azure VMware Solution private cloud. The ExpressRoute Premium SKU is required to enable Global Reach.



Azure VMware Solution private clouds require, at minimum, a /22 CIDR network address block for subnets. To connect to on-premises environments and virtual networks, this must be a non-overlapping network address block.

#### NOTE

To learn about network planning for Azure VMware Solution, see [Networking checklist for Azure VMware Solution](#).

## Step 2: Create an Azure VMware Solution private cloud

With its network and IP address planning completed, Contoso will next focus on setting up the Azure VMware Solution service in the West US Azure region. By using Azure VMware Solution, Contoso can deploy a vSphere cluster in Azure.

An Azure VMware Solution private cloud is an isolated, VMware software-defined datacenter that supports ESXi hosts, vCenter, vSAN, and NSX. The stack runs on dedicated and isolated bare-metal hardware nodes in an Azure region. The minimum initial deployment for an Azure VMware Solution private cloud is three hosts. Additional hosts can be added one at a time, up to a maximum of 16 hosts per cluster.

For more information, see [Azure VMware Solution preview private cloud and cluster concepts](#).

Azure VMware Solution private clouds are managed through the Azure VMware Solution portal. Contoso has its own vCenter server in its own management domain.

To learn how to create Azure VMware Solution private clouds, see [Deploy an Azure VMware Solution private cloud in Azure](#).

1. The Contoso team first registers the Azure VMware Solution provider with Azure by running the following command:

```
az provider register -n Microsoft.AVS --subscription <your subscription ID>
```

2. In the Azure portal, the team creates the Azure VMware Solution private cloud by providing the networking information from the plan. The team then selects **Review + create**. This step takes about two hours.

**AVS Private cloud**

**\* Basics** Tags Review + create

Azure settings

Subscription \*  Resource group \*  Create new

Location \*

General

Resource name \*  SKU \*  Hosts \*  vCenter admin password  Confirm vCenter admin password  NSX-T Manager password  Confirm NSX-T Manager password

Networking

Address block \*

**Review + create** Previous Next : Tags >

3. The team verifies that the Azure VMware Solution private cloud deployment is complete by going to the resource group and selecting the private cloud resource. The status is displayed as *Succeeded*.

**ContosoPrivateCloud**

Home > ContosoResourceGroup > ContosoPrivateCloud

Overview

Status **Succeeded**

Resource group (change)  
ContosoResourceGroup

Hosts  
Cluster-1: 3

Primary peering subnet  
10.210.3.8/30

Secondary peering subnet  
10.210.3.12/30

Subscription (change)  
Contoso

Subscription ID

Private Cloud Management network  
10.210.0.0/24

vMotion network  
10.210.1.0/24

VM Workload network  
10.210.2.0/24

Tags (change)  
Click here to add tags

### Step 3: Configure networking

An Azure VMware Solution private cloud requires a virtual network. Because Azure VMware Solution doesn't support an on-premises vCenter during preview, Contoso requires additional steps for integration with its on-premises environment. By setting up an ExpressRoute circuit and a virtual network gateway, the team connects its virtual networks to the Azure VMware Solution private cloud.

For more information, see [Configure networking for your VMware private cloud in Azure](#).

1. The Contoso team first creates a virtual network with a gateway subnet.

#### IMPORTANT

The team must use an address space that *does not* overlap with the address space that it used when it created the private cloud.

2. The team creates the ExpressRoute VPN gateway, making sure to select the correct SKU, and then selects **Review + create**.

#### Create virtual network gateway

##### Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription \*

Contoso

Resource group ⓘ

ContosoResourceGroup (derived from virtual network's resource group)

##### Instance details

Name \*

PrivateCloudGateway

Region \*

East US

Gateway type \* ⓘ

VPN  ExpressRoute

SKU \* ⓘ

Standard

Virtual network \* ⓘ

PrivateCloudVNET

[Create virtual network](#)

ⓘ Only virtual networks in the currently selected subscription and region are listed.

Gateway subnet address range \* ⓘ

172.29.1.0/24

172.29.1.0 - 172.29.1.255 (256 addresses)

##### Public IP address

Public IP address \* ⓘ

Create new  Use existing

Public IP address name \*

PrivateCloudGatewayIP

Public IP address SKU

Basic

Assignment

Dynamic  Static

Azure recommends using a validated VPN device with your virtual network gateway. To view a list of validated devices and instructions for configuration, refer to Azure's [documentation](#) regarding validated VPN devices.

**Review + create**

< Previous

Next : Tags >

Download a template for automation

3. The team gets the authorization key to connect ExpressRoute to the virtual network. The key is found on the connectivity screen of the Azure VMware Solution private cloud resource in the Azure portal.

The screenshot shows the Azure portal interface for a private cloud named 'ContosoPrivateCloud'. The left sidebar has sections for Overview, Activity log, Access control (IAM), Tags, and Diagnose and solve problems. Under Settings, there are Locks and Export template. Under Manage, Connectivity is selected, followed by Identity and Scale private cloud. The main content area is titled 'ExpressRoute' and shows two tabs: ExpressRoute ID and Private peering ID. Both tabs have dropdown menus showing '/subscriptions/' and '/resourceGroups/tnt72-cust-p01-rstn01/provide...'. Below these tabs is a button labeled '+ Request an authorization key'. A table lists a single row with 'Name' as 'privatecloudkey' and 'Key' as '442cb5d8'. There are icons for copy, delete, and more options next to the key value.

4. The team connects the ExpressRoute to the VPN gateway that connects the Azure VMware Solution private cloud to the Contoso virtual network. It does this by creating a connection in Azure.

 **Add connection**

PrivateCloudGateway |  Directory: Microsoft

**Important** Ensure that the ExpressRoute associated with this authorization is provisioned by the provider before redeeming the authorization.

**Name \***  
privatecloud-connection 

**Connection type**   
ExpressRoute 

**Redeem authorization** 

**\*Virtual network gateway**   
PrivateCloudGateway 

**Authorization key \***  
442cb5d8  

**Peer circuit URI \***  
/subscriptions/750a6f9e...  

**Subscription**   


**Resource group**   
ContosoResourceGroup   
[Create new](#)

**Location**   
East US 

**OK**

For more information, see [Learn how to access an Azure VMware Solution private cloud](#).

#### Step 4: Migrate by using VMware HCX

To move VMware VMs to Azure using HCX, the Contoso team will need to follow these high-level steps:

- Install and configure VMware HCX.
- Perform migrations to Azure by using HCX.

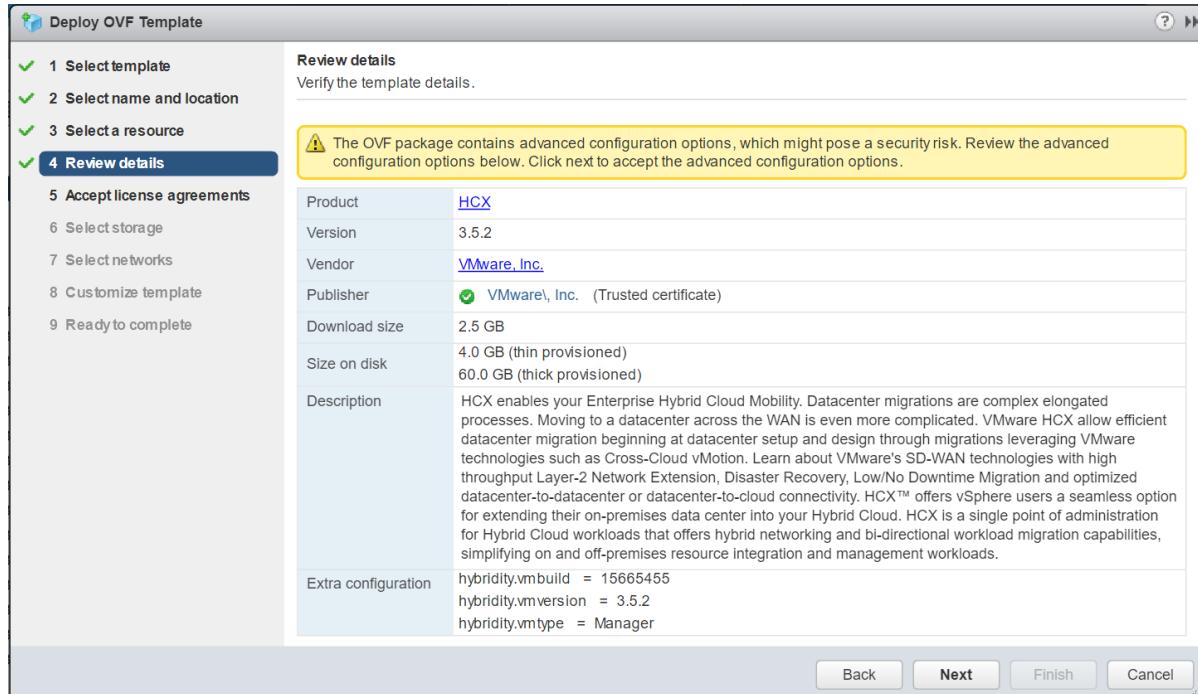
For more information, see [Install HCX for Azure VMware Solution](#).

#### Install and configure VMware HCX for the public cloud

VMware HCX is a VMware product that's part of the Azure VMware Solution default installation. HCX Advanced is installed by default, but it can be upgraded to HCX Enterprise as additional features and functionality are required.

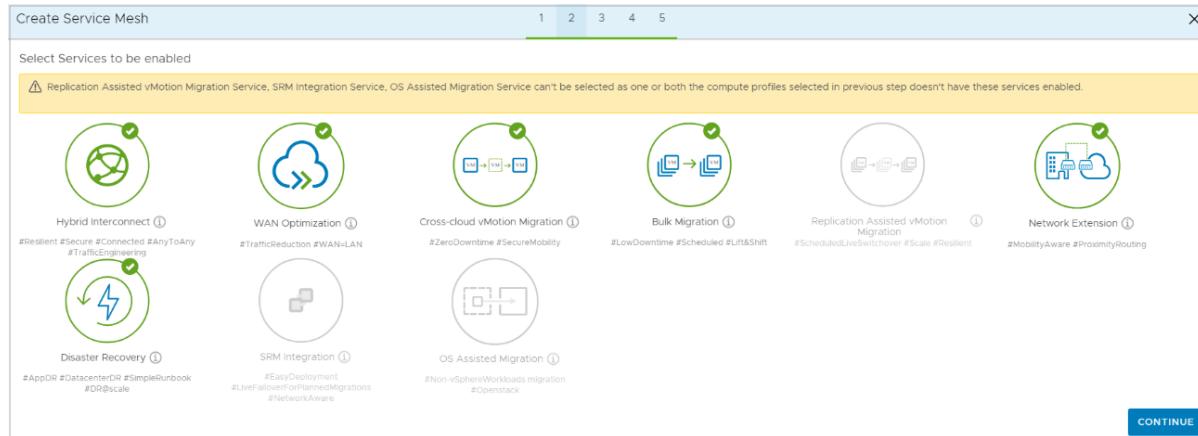
Azure VMware Solution automates the cloud manager component of HCX in Azure VMware Solution. It provides the customer activation keys and download link to the connector HCX appliance that must be configured on the on-premises side and in a customer's vCenter domain. These elements are then paired with the Azure VMware Solution cloud appliance, so that customers can take advantage of services such as migration and L2 stretch.

- The Contoso team is deploying the HCX by using an OVF package that's provided by VMware.



To install and configure HCX for your Azure VMware Solution private cloud, see [Install HCX for Azure VMware Solution](#).

- As the team is configuring HCX, it has chosen to enable migration and other options, including disaster recovery.

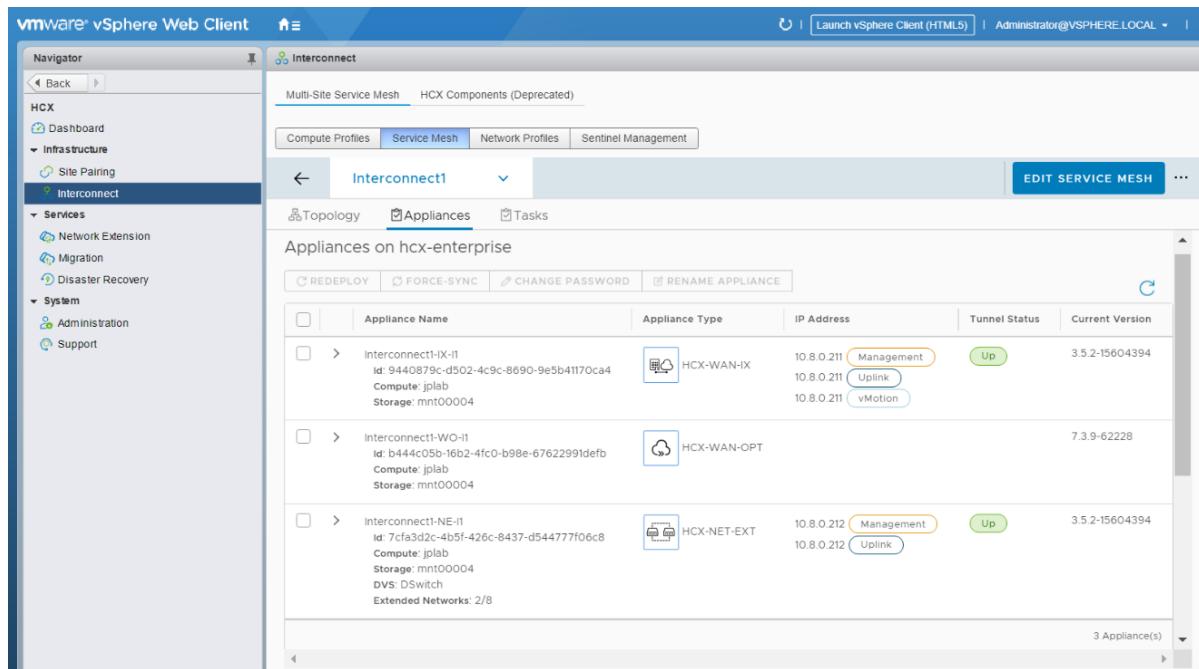


For more information, see [HCX installation workflow for HCX public clouds](#).

#### Migrate VMs to Azure by using HCX

When both the on-premises datacenter (source) and the Azure VMware Solution private cloud (destination) are configured with the VMware cloud and HCX, Contoso can begin migrating its VMs. The team can move VMs to and from VMware HCX-enabled datacenters by using multiple migration technologies.

- Contoso's HCX application is online, and the status is green. The team is now ready to migrate and protect Azure VMware Solution VMs by using HCX.



### VMware HCX bulk migration

This migration method uses the VMware vSphere replication protocols to move multiple VMs simultaneously to a destination site. Benefits include:

- This method is designed to move multiple VMs in parallel.
- The migration can be set to finish on a predefined schedule.
- The VMs run at the source site until failover begins. The service interruption is equivalent to a reboot.

### VMware HCX vMotion live migration

This migration method uses the VMware vMotion protocol to move a single VM to a remote site. Benefits include:

- This method is designed to move one VM at a time.
- There's no service interruption when the VM state is migrated.

### VMware HCX cold migration

This migration method uses the VMware near-field communication protocol. The option is automatically selected when the source VM is powered off.

### VMware HCX Replication-assisted vMotion

VMware HCX RAV combines the benefits of VMware HCX bulk migration, which include parallel operations, resiliency, and scheduling, with the benefits of VMware HCX vMotion migration, which include zero downtime during VM state migration.

## Additional resources

For additional VMware technical documentation, see:

- [VMware HCX documentation](#)
- [Migrate virtual machines by using VMware HCX](#)

# Move on-premises Remote Desktop Services to Azure Windows Virtual Desktop scenario

11/9/2020 • 11 minutes to read • [Edit Online](#)

Windows Virtual Desktop is a comprehensive desktop and application virtualization service running in the cloud. It's the only virtual desktop infrastructure (VDI) that delivers simplified management, Windows 10 Enterprise multi-session optimizations for Microsoft 365 Apps for enterprise, and support for Remote Desktop Services (RDS) environments. Deploy and scale Windows desktops and applications on Azure in minutes, and get built-in security and compliance features.

MIGRATION OPTIONS	OUTCOME
Azure Migrate	Assess and migrate on-premises RDS environments. Run workloads by using Azure Windows Virtual Desktop. Manage Windows Virtual Desktop with <a href="#">Windows Virtual Desktop management UX</a> .

## NOTE

This article focuses on using Windows Virtual Desktop in Azure to move an on-premises RDS environment to Azure.

## Business drivers

Working closely with business partners, the Contoso IT team will define the business drivers for a VDI migration to Azure. These drivers might include:

- **Current environment end-of-life:** A datacenter is out of capacity when it reaches the end of a lease or is closing down. Migrating to the cloud provides virtually unlimited capacity. Current software might also be reaching its end of life where it has become necessary to upgrade the software running Contoso's current VDI solution.
- **Multi-session Windows 10 VDI:** Provide Contoso users with the only multi-session Windows 10 desktop virtualized in the cloud that's highly scalable, up to date, and available on any device.
- **Optimize for Microsoft 365 Apps for enterprise:** Deliver the best Microsoft 365 Apps for enterprise experience, with multi-session virtual desktop scenarios providing the most productive virtualized experience for Contoso's users.
- **Deploy and scale in minutes:** Quickly virtualize and deploy modern and legacy desktop applications to the cloud in minutes with unified management in the Azure portal.
- **Secure and productive on Azure and Microsoft 365:** Deploy a complete, intelligent solution that enhances creativity and collaboration for everyone. Shift to Microsoft 365 and get Office 365, Windows 10, and Enterprise Mobility + Security.

## RDS on-premises to Windows Virtual Desktop in the cloud goals

With the business drivers in mind, Contoso has pinned down goals for this migration:

- Modernize the virtual desktop environment for the cloud.
- Take advantage of existing Microsoft 365 licenses.

- Improve security of corporate data when users work remotely.
- Optimize the new environment for cost and growth.

These goals support the decision to use Windows Virtual Desktop and validate it as the best migration method for Contoso.

## Benefits of running Windows Virtual Desktop in Azure

Using Windows Virtual Desktop in Azure, Contoso can now seamlessly run, manage, and scale its VDI solution quickly and easily. The company also can provide an optimized multi-session Windows 10 environment to its users.

Contoso will capitalize on existing Microsoft 365 licenses while using the scale, performance, security, and innovation of Azure.

Additional benefits might include:

- Access to Windows Virtual Desktop from anywhere.
- Optimized Microsoft 365 Apps for enterprise environment.
- Windows Virtual Desktop for dev/test environments.

## Solutions design

After pinning down goals and requirements, Contoso designs and reviews a deployment solution and identifies the migration process.

### Current architecture

RDS is deployed to an on-premises datacenter. Microsoft 365 is licensed and in use by the organization.

### Proposed architecture

- Sync Active Directory or Azure Active Directory Domain Services.
- Deploy Windows Virtual Desktop to Azure.
- Migrate on-premises RDS servers to Azure.
- Convert user profile disks (UPDs) to FSLogix profile containers.

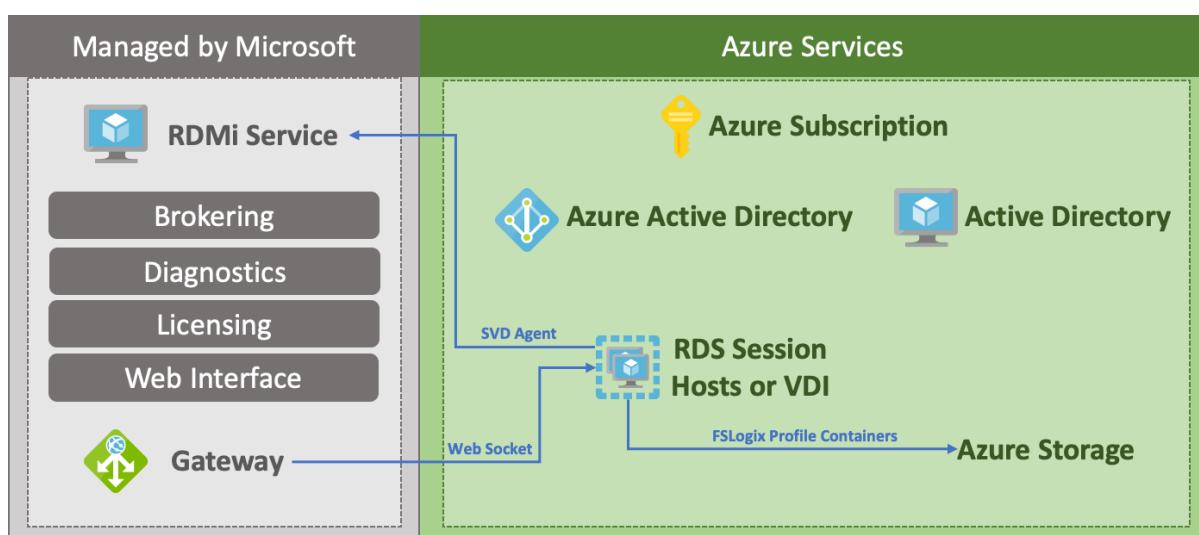


Figure 1: Proposed architecture.

## Solution review

Contoso evaluates the proposed design by putting together a list of pros and cons.

CONSIDERATION	DETAILS
Pros	<p>Windows 10 Enterprise multi-session environment.</p> <p>Cloud-based, allowing access from anywhere.</p> <p>Take advantage of other Azure services like Azure Files within the Windows Virtual Desktop environment.</p> <p>Optimized for the Microsoft modern desktop.</p>
Cons	<p>To fully optimize for Azure, Contoso will have to rebuild Windows 10 images optimized for multiuser sessions.</p> <p>Windows Virtual Desktop doesn't support user profile disks, so UPDs must be migrated to FSLogix profile containers.</p>

## Migration process

Contoso will move VMs to Windows Virtual Desktop in Azure by using the Lakeside assessment tool and Azure Migrate. Contoso will need to:

- Run the assessment tool against its on-premises RDS infrastructure to establish the scale of the Windows Virtual Desktop deployment in Azure.
- Migrate to Windows Virtual Desktop via either Windows 10 Enterprise multi-session or persistent virtual machines.
- Optimize the Windows Virtual Desktop multi-session by scaling up and down as needed to manage costs.
- Virtualize applications and assign users as needed to continue to secure and manage the Windows Virtual Desktop environment.

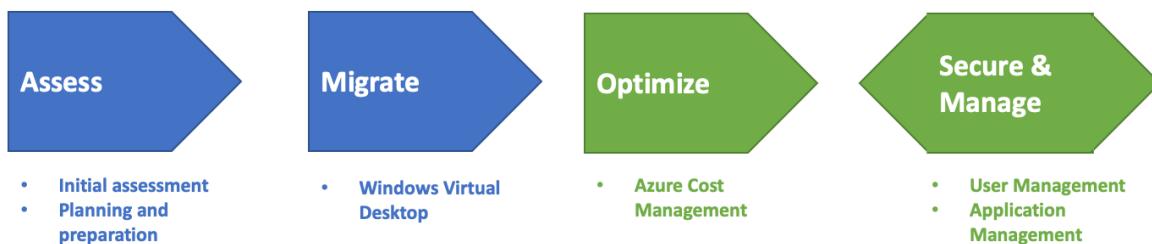


Figure 2: The migration process.

## Scenario steps

1. Assess the current RDS environment.
2. Create the VDI and new images in Azure and migrate and persist VMs to Azure.
3. Convert UPDs to FSLogix profile containers.
4. Replicate any persistent VMs to Azure.

## Step 1: Assess the current on-premises environment

Contoso will provision the Windows Virtual Desktop service in the **East US 2** Azure region. With Windows Virtual Desktop, Contoso can provision virtual machines, host pools, and create application groups. Windows Virtual Desktop also configures an availability set for all the servers in the Windows Virtual Desktop solution. Windows Virtual Desktop allows Contoso to create a high-available VDI environment and to scale up and down quickly as needed.

**NOTE**

Contoso reviewed two scenarios during the assessment: multi-session (shared) instances of RDS and persistent (or user-dedicated) virtual machines.

1. Make sure that domain services, either Active Directory or Azure Active Directory Domain Services, are synchronized with Azure Active Directory (Azure AD). Ensure the domain service is accessible from the Azure subscription and virtual network to be connected where Windows Virtual Desktop will be deployed.

**NOTE**

Learn more about [Azure AD Connect](#) for synchronizing Active Directory on-premises with Azure AD.

**NOTE**

Learn about provisioning [Azure Active Directory Domain Services](#) and synchronizing Azure AD to it.

2. Create a new Azure Migrate project.

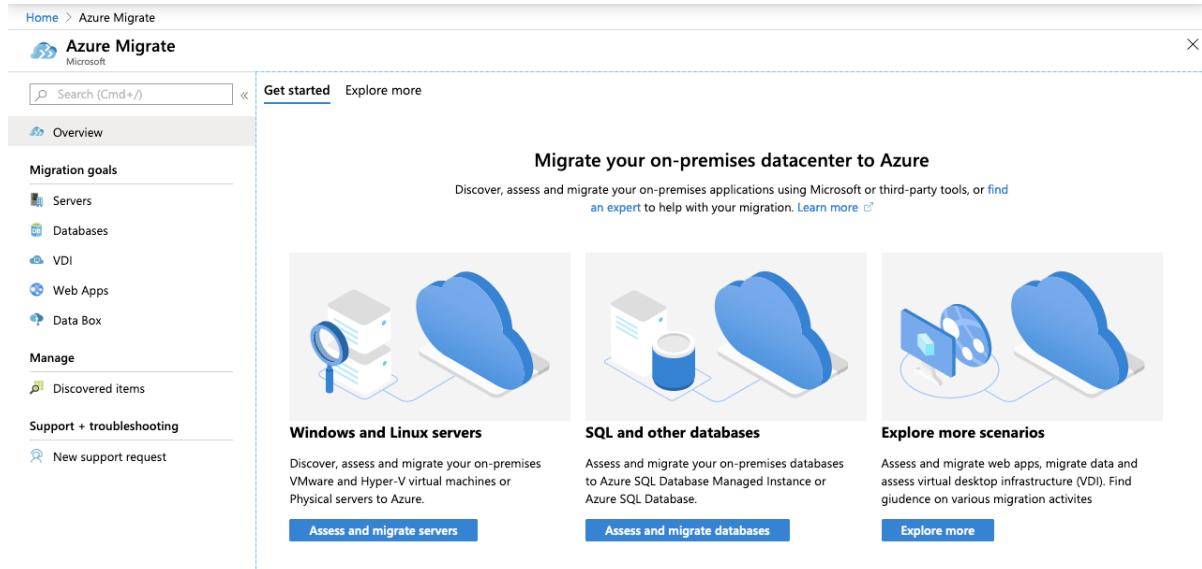


Figure 3: Creating a new Azure Migrate project.

3. Select the option to assess and migrate servers, select VDI, and add a tool.

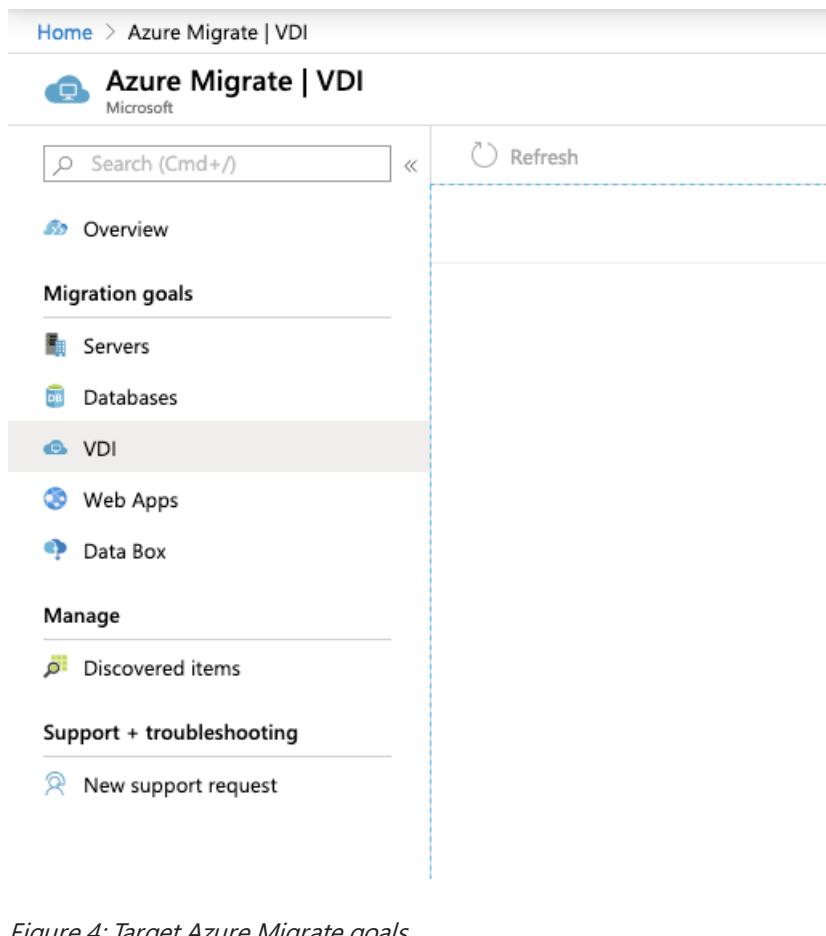


Figure 4: Target Azure Migrate goals.

- Set the subscription, resource group, project name, and geography for the migrate job data.

The screenshot shows the 'Add a tool' page for creating a migration project. At the top, there are tabs: 'Migrate project' (selected), 'Select assessment tool', 'Select migration tool', and 'Review + add tool(s)'. Below this, a note says: 'An Azure Migrate project is used to store the discovery, assessment and migration metadata reported by your on-premises environment. Select a subscription and resource group in your preferred geography to create the migrate project.' There are fields for 'Subscription' (dropdown menu) and 'Resource group' (dropdown menu showing '(New) Contoso-WVD' with a 'Create new' link). Under 'PROJECT DETAILS', there are fields for 'Migrate project' (dropdown menu showing 'RDS-to-WVD') and 'Geography' (dropdown menu showing 'United States').

Figure 5: Adding job data to the migration.



- Select Lakeside: SysTrack as the assessment tool.

6. Select Azure Migrate: Server Migration as the migration tool.

7. Add the tools to the migration project.

The screenshot shows the 'Add a tool' page with the following navigation bar: Home > Azure Migrate | VDI > Add a tool. Below the navigation is a section titled 'Add a tool' with tabs: Migrate project, Select assessment tool, Select migration tool, and Review + add tool(s). The 'Review + add tool(s)' tab is selected. A 'Settings' section displays the following configuration:

Setting	Value
Subscription	-subscription name-
Resource group	(new) Contoso-WVD
Geography	United States
Assessment tool	Lakeside: SysTrack
Migration tool	Azure Migrate: Server Migration
Migrate project	(new) RDS-to-WVD

Figure 6:

Adding tools to the migration.

8. Start the assessment of the current environment by selecting Register with Azure Migrate in the Lakeside tool.

The screenshot shows the 'Assessment tools' section for the Lakeside tool. It includes a logo and the text 'Lakeside'. Below it is a button labeled 'Register with Azure Migrate\*' which is highlighted with a red box. The page also contains sections for 'Quick start' (with '1: Register' and 'Connect' steps), and a link to 'Add more assessment tools? Click here.'

Figure 7: Assessing the current environment.

9. Contoso connects Azure Migrate and Lakeside, and accepts any requested permissions.

## Windows Virtual Desktop Assessment with SysTrack



*Figure 8: Connecting Azure to Lakeside.*

10. Contoso continues with the Lakeside tool to create a new tenant and start assessing the current on-premises RDS environment. From the dashboard, Contoso can access the deployment guide, download the assessment client to deploy to the current environment, and review the data collected from these agents.

# Contoso

Assessment | Setup

- 1 Getting Started**
  -  Quick Start Guide
  -  Download Assessment Client
    - \* This client install has been configured specifically for your assessment.
  -  Agent Collection Status Summary
- 2 Review Collected Data**
  -  Visualizer - Enterprise
  -  Visualizer - Desktop
  -  Visualizer - Server
  -  Visualizer - Persona
- 3 Report on WVD**
  -  WVD Migration Guide
- 4 Resolve**
  -  Resolve
- 5 AppVision**
  -  AppVision
- 6 Configure**
  -  Configure
- 7 Reports Center**
  -  Report Center
- 8 Dashboards**
  -  Dashboards
- 9 Dashboard Builder**
  -  Dashboard Builder

**Kits**

 SysTrack Kits

**AIOps**

 AIOps

Figure 9: The Lakeside dashboard.

11. After an adequate amount of data is captured, Contoso reviews the assessment data to determine the best migration path. This assessment data includes the raw assessment data from the desktops data and the data broken into different user personas. This information includes the:

- Number of users in each persona.
- Applications in use by users.
- Resource consumption by user.
- Resource utilization averages by user persona.
- VDI server performance data.
- Concurrent user reports.
- Top software packages in use.

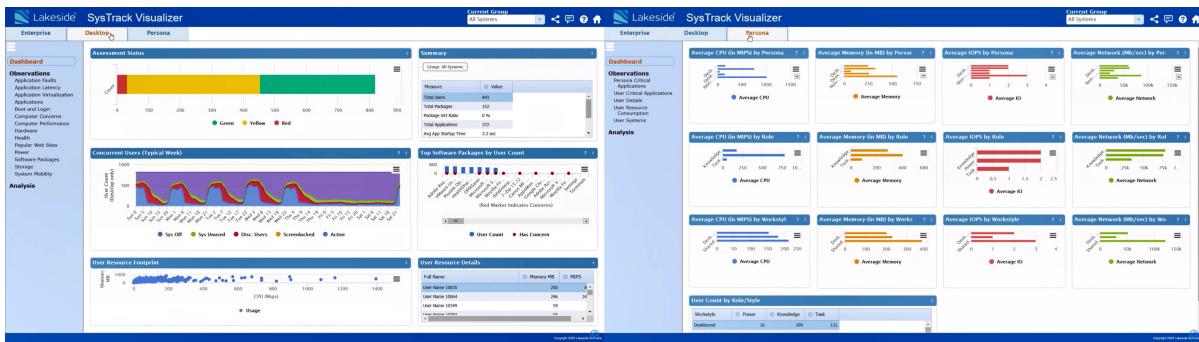


Figure 10: Lakeside dashboard reports.

The data is analyzed by Contoso to determine the most cost-effective use of both pooled Windows Virtual Desktop resources and personal Windows Virtual Desktop resources.

#### NOTE

Contoso will also need to migrate application servers to Azure to get the company closer to the Windows Virtual Desktop environment and reduce network latency for its users.

## Step 2: Create the Windows Virtual Desktop environment for pooled desktops

Using the Azure portal, Contoso will create a Windows Virtual Desktop environment to use for pooled resources. Later, it will go through the migration steps to attach personal desktops to the same environment.

1. Contoso selects the correct subscription, and creates a new Windows Virtual Desktop host pool.

The figure shows a screenshot of the 'Windows Virtual Desktop - Provision a host pool' page in the Azure portal. The URL is 'Home > New > Windows Virtual Desktop - Provision a host pool'. The title is 'Windows Virtual Desktop - Provision a host pool' with a Microsoft logo and a 'Create' button. Below the title, there are tabs for 'Overview' (which is selected) and 'Plans'. The 'Overview' section contains the following text: 'Windows Virtual Desktop allows you to deploy and scale Windows and Office on Azure in minutes, with built-in security and compliance.' It also lists benefits: 'Windows Virtual Desktop includes the following benefits:' followed by a bulleted list of features including compatibility with Microsoft Store, Extended Security Updates, and deep integration with Microsoft 365.

Figure 11: A new Windows Virtual Desktop host pool.

2. Specify the subscription, resource group, and region. Then select the name for the host pool, desktop type, and default desktop users. Desktop type is set to **Pooled** because Contoso is starting with a new shared environment for some of its users. Default desktop users can be left blank. Move on to configure the virtual machines.

## Create a host pool

[Basics](#)   [Virtual Machines](#)   [Workspace](#)   [Tags](#)   [Review + create](#)

### Project details

Subscription \* ⓘ

-subscription name-

Resource group \* ⓘ

Contoso-WVD

[Create new](#)

Host pool name \*

ContosoWVD

Location \* ⓘ

(US) East US 2

Metadata will be stored in East US 2

### Host pool type

If you select pooled (shared), users will still be able to access their personalization and user data, using FSLogix.

Host pool type \*

Pooled

Max session limit ⓘ

150

Load balancing algorithm ⓘ

Breadth-first

Figure 12: Prerequisites for configuring virtual machines.

- Contoso configures the VM and chooses a custom size by selecting **Change size** or using the default.
- Windows Virtual Desktop is chosen as the VM name prefix for these pooled desktops.
- Because Contoso is creating the pooled servers to use the new Windows 10 Enterprise multi-session functionality for the virtual machine settings, leave the image source set to **Gallery**. This option enables Contoso to select the Windows 10 Enterprise multi-session image for the VMs.
- Based on the personas of the users from the Lakeside assessment, Contoso sets the total users to **150**.
- Other settings include the disk type, an AD domain join UPN field, an admin password, an optional OU path to which machines are added, the virtual network, and a subnet for adding servers.

## Create a host pool

[Basics](#)   [Virtual Machines](#)   [Workspace](#)   [Tags](#)   [Review + create](#)

Host pools are a collection of one or more identical virtual machines within Windows Virtual Desktop environments. Here you give details to create a resource group with virtual machines in an Azure subscription. [Learn more](#) ⓘ

Add virtual machines

No  Yes

Resource group

Contoso-WVD

Virtual machine location ⓘ

(US) East US 2

Virtual machine size \* ⓘ

**Standard D4s v3**

4 vCPU's, 16 GiB memory

[Change size](#)

Number of VMs \*

10

Name prefix \*  ✓

i Session host name must be unique within the Resource Group.

Image type  ✓

Image \* (i)  ✓

[Browse all images and disks](#)

OS disk type \* (i)  ✓

Use managed disks (i)  Yes  No

**Network and security**

\*Virtual network (i)  ✓

Subnet (i)  ✓

Public IP (i)  Yes  No

Network security group (i)  ✓

Public inbound ports (i)  Yes  No

Inbound ports to allow  ✓

i All traffic from the internet will be blocked by default.

Specify domain or unit (i)  Yes  No

Domain to join \* (i)  ✓

Organizational Unit path (i)

**Administrator account**

AD domain join UPN \* (i)  ✓

Password \* (i)  ✓

Confirm password \* (i)  ✓

Review + create < Previous Next: Workspace >

Figure 13: Configuring virtual machines.

**NOTE**

Contoso can't create a new virtual network at this step. Before reaching this step, Contoso should have already created a virtual network that has access to Active Directory.

**NOTE**

Contoso can't use a user account that requires multi-factor authentication in this step. If Contoso plans to use multi-factor authentication for its users, it will need to create a service principal for this purpose.

- Contoso performs one more validation of the Windows Virtual Desktop settings, and creates the new environment of pooled Windows Virtual Desktop virtual machines.

Home > Windows Virtual Desktop - Provision a host pool > Create Windows Virtual Desktop - Provision a host pool

### Create Windows Virtual Desktop - Provision a host pool

Basics Configure virtual machines Virtual machine settings Windows Virtual Desktop information **Review + create**

**ERRORS**  
The template deployment 'rds.wvd-provision-host-pool-20200504235504' is not valid according to the validation procedure. The tracking id is 'd4f8e25e-fc65-4e37-8358-76a91806cbcd'. See inner errors for details.

**PRODUCT DETAILS**  
Windows Virtual Desktop - Provision a host pool by Microsoft [Terms of use](#) | [Privacy policy](#)

**TERMS**  
By clicking "Create", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed above; (b) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), with the same billing frequency as my Azure subscription; and (c) agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party offerings. See the [Azure Marketplace Terms](#) for additional details.

Basics	
Subscription	-subscription name-
Resource group	Contoso-WVD
Default desktop users	-
Service metadata location	United States
Configure virtual machines	
Create an Availability Set	Yes
Usage Profile	Medium
Total users	150
Virtual machine size	Standard_D4s_v3
Virtual machine name prefix	WVD-
Virtual machine settings	
Image source	Gallery
Image OS version	Windows 10 Enterprise multi-session with Office 365 ProPlus
Disk Type	Premium SSD
AD domain join UPN	user@contoso.com
Admin Password	*****
Specify domain or OU	No
Virtual network	vnet-01
vmSubnet	default
Address prefix (vmSubnet)	10.0.0.0/24
Windows Virtual Desktop information	
Windows Virtual Desktop tenant group name	Contoso Default Group
Windows Virtual Desktop tenant name	Contoso
Windows Virtual Desktop tenant RDS OwnerUPN	
UPN	user@contoso.com
Password	*****

Figure 14: Reviewing and creating virtual machines.

## Step 3: Convert the UPDs to FSLogix profile containers

Because Windows Virtual Desktop doesn't support user profile disks (UPDs), Contoso needs to convert all the UPDs to FSLogix via the [FSLogixMigration PowerShell module](#).

After Contoso imports the FSLogixMigration module, it runs the following PowerShell cmdlets to migrate from UPDs to FSLogix.

### IMPORTANT

The PowerShell modules for Hyper-V, Active Directory, and Pester are prerequisites to running the cmdlets to convert UPDs to FSLogix.

A UDP conversion:

```
Convert-RoamingProfile -ParentPath "C:\Users\" -Target "\\\Server\FSLogixProfiles$" -MaxVHDSIZE 20 -  
VHDLogicalSectorSize 512
```

A roaming profile conversion:

```
Convert-RoamingProfile -ProfilePath "C:\Users\User1" -Target "\\\Server\FSLogixProfiles$" -MaxVHDSIZE 20 -  
VHDLogicalSectorSize 512 -VHD -IncludeRobocopyDetails -LogPath C:\temp\Log.txt
```

At this point, the migration has enabled using pooled resources with Windows 10 Enterprise multi-session. Contoso can begin to deploy the necessary applications to the users who will use Windows 10 Enterprise multi-session.

But now Contoso must migrate the persistent virtual machines to Azure.

## Step 4: Replicate and persist VMs to Windows Virtual Desktop

The next step in the migration process for Contoso is to migrate its persistent virtual machines to Windows Virtual Desktop. To do this, Contoso goes back to the Azure Migrate: Server Migration job it created at the beginning of the process.

1. Contoso starts by selecting **Discover** in the Azure Migrate: Server Migration tools.

The screenshot shows the Azure Migrate: Server Migration interface. On the left, there's a sidebar with options for VDI, Web Apps, and Data Box under 'Manage', and Discovered items and New support request under 'Support + troubleshooting'. The main area is titled 'Migration tools' and features the 'Azure Migrate: Server Migration' logo. It has four tabs: Discover (which is highlighted with a red box), Replicate, Migrate, and Overview. Below the tabs, there's a table with four rows: Discovered servers (36520), Replicating servers (3), Test migrated servers (2), and Migrated servers (1). At the bottom, a yellow lightning bolt icon indicates the 'Next step: You can start migrating the replicating servers to Azure'.

	Discovered servers	36520
	Replicating servers	3
	Test migrated servers	2
	Migrated servers	1

Figure 15: Discovering a server migration.

2. Contoso converts an appliance in its environment that's going to manage the replication of the machines to Windows Virtual Desktop. Ensure that the target region is set to **East US 2**, where the Windows Virtual Desktop environment was created.

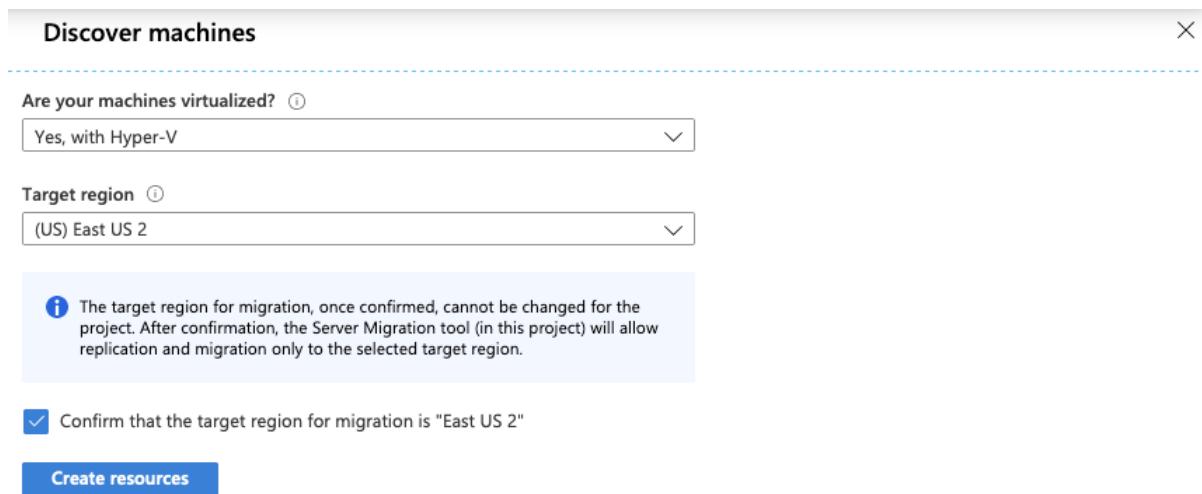


Figure 16: Converting an appliance.

3. The replication provider is downloaded, installed, and registered to the Azure Migrate project to start the replication to Azure.

**Discover machines**

Are your machines virtualized? ⓘ

Yes, with Hyper-V

Target region ⓘ

(US) East US 2

**Prepare for replication by downloading and installing the replication provider software on your Hyper-V hosts. Follow the steps below to setup and configure Hyper-V host servers.**

**1. Prepare Hyper-V host servers.**  
Download the Hyper-V replication provider(AzureSiteRecoveryProvider.exe) software installer. Use the installer to install the replication provider on the Hyper-V servers.  
Download the registration key file and use it to register the Hyper-V host to this Azure Migrate project.  
[Download](#)

**2. Finalize registration.**  
Prepare for replication by finalizing registration for the Hyper-V hosts.

Registered Hyper-V hosts 0 (Connected) [Why do I not see any Hyper-V host?](#)

**⚠️** At least one Hyper-V host must be registered to proceed with this step. Complete step 1 to proceed.

[Finalize registration](#)

Figure 17: Prerequisites for replicating to Azure.

4. The replication of the hosts into Azure Blob storage is now started. Contoso can continue to let the replication occur until it's ready to test the VMs and then migrate them into production.
- As machines start running in Azure, Contoso makes sure to install the [Windows Virtual Desktop VM agent](#) on each machine.
- As a part of the installation, enter the registration token for the Windows Virtual Desktop environment to associate the server with the correct environment.
- The registration token can be obtained by using the following commands:

```
Export-RDSRegistrationInfo -TenantName "Contoso" -HostPoolName "ContosoWVD" | Select-Object -ExpandProperty Token > .\registration-token.txt
```

#### NOTE

Contoso can also automate this process by using `msiexec` commands and passing in the registration token as a variable.

- As the last step before the final migration, Contoso selects the **Users** item in the Azure Windows Virtual Desktop settings to map the servers to their respective users and groups.

Name	Host pool	Type	Resource
0224Apps	0224HP	RemoteApp	0224RG
0224HP-DAG	0224HP	Desktop	0224RG
<input checked="" type="checkbox"/> Workapps	0224HP	RemoteApp	0224RG
0226RG-DAG	0226RG	Desktop	0226RG
0301RAG	0301HP	RemoteApp	0301RG
03162HP-DAG	03162HP	Desktop	0316RG
demohp-DAG	demohp	Desktop	0414RG
0422hp-DAG	0422hp	Desktop	0422rg
0422testhp	0422testhp	Desktop	0422rg
pdtestrag	0422hp	RemoteApp	0422rg
testrag	0422testhp	RemoteApp	0422rg

Figure 18: The last step prior to the final migration.

After host pools are assigned to users, Contoso finalizes the migration of those machines and continues to gradually migrate the rest of the on-premises VDI hosts to Azure.

## Review the deployment

With the virtual desktops and application servers now running in Azure, Contoso now needs to fully operationalize and secure the deployment.

### Security

The Contoso security team reviews the Azure VMs to determine any security issues. To control access, the team reviews the network security groups (NSGs) for the VMs. NSGs are used to ensure that only traffic allowed to the application can reach it. The team also considers securing the data on the disk by using Azure Disk Encryption and Azure Key Vault.

For more information, see [Security best practices for IaaS workloads in Azure](#).

## Business continuity and disaster recovery

For business continuity and disaster recovery (BCDR), Contoso backs up the data on the VMs by using Azure Backup to keep data safe. For more information, see [An overview of Azure VM backup](#).

### Licensing and cost optimization

- Microsoft 365 licenses are used for the desktop deployments.
- Contoso will enable [Azure Cost Management + Billing](#) to help monitor and manage the Azure resources.
- Contoso has existing licensing for its VMs and will take advantage of the Azure Hybrid Benefit for application servers. Contoso will convert the existing Azure VMs to take advantage of this pricing.

## Conclusion

In this article, Contoso moved its RDS deployment to Windows Virtual Desktop hosted in Azure.

# VMware host migration best practices for Azure

11/9/2020 • 2 minutes to read • [Edit Online](#)

Migrating VMware host to Azure can accelerate the standard methodology outlined in the Cloud Adoption Framework, and pictured here.

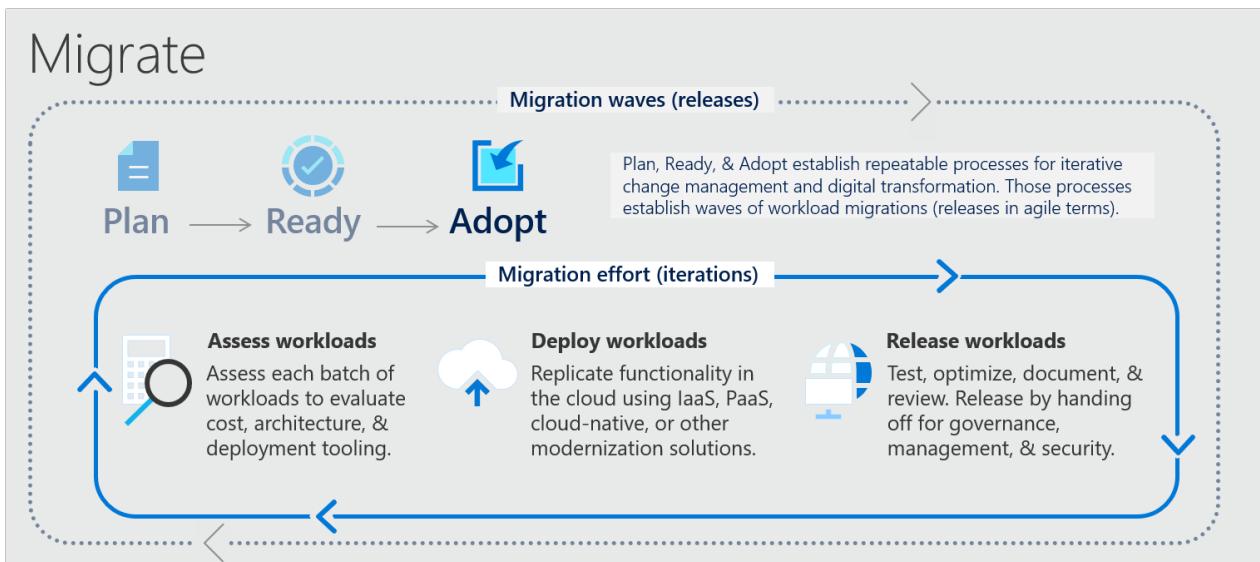


Figure 1

The table of contents on the left outlines best practices across multiple Microsoft web properties. These best practices can guide the execution of your VMware host migration to Azure VMware Solution. Bookmark this page to quickly reference the full list of best practices.

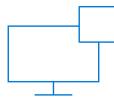
# Migrate or deploy Windows Virtual Desktop instances to Azure

11/9/2020 • 2 minutes to read • [Edit Online](#)

Migrating an organization's end-user desktops to the cloud is a common scenario in cloud migrations. Doing so helps improve employee productivity and accelerate the migration of various workloads to support the organization's user experience.

## Strategy and motivations

Virtual desktop migrations are motivated by a few common target outcomes, as shown and listed here:



Productivity on a PC, phone, tablet, or browser



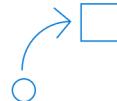
Safe access to corporate data and apps



Support end users during your cloud migration



Optimize costs of enabling your workforce



Empower IT to transform the workplace

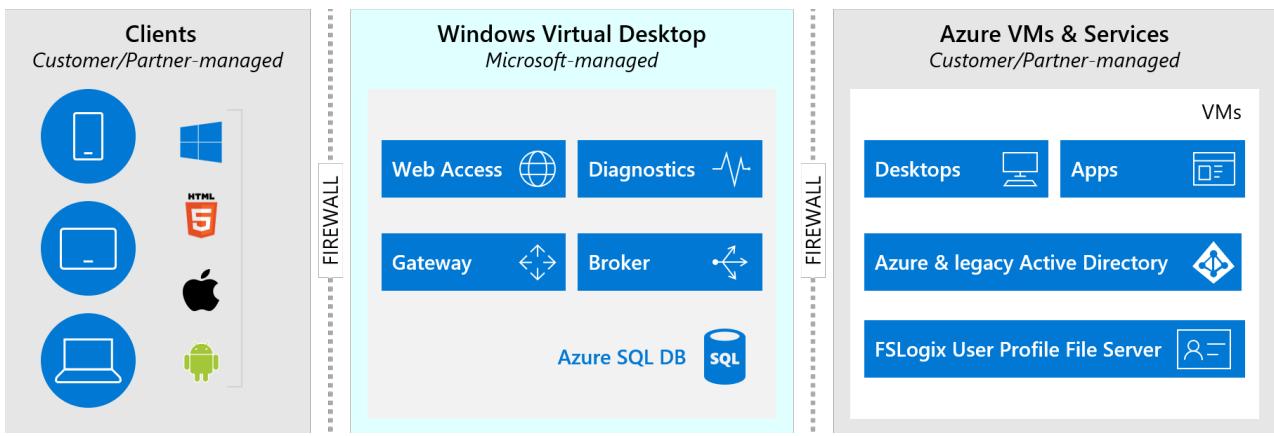
- Organizations want to extend productivity to PCs, phones, tablets, or browsers that might not be under the direct control of the IT team.
- Employees need to access corporate data and applications from their devices.
- As workloads are migrated to the cloud, employees need more support for a low-latency, more optimized experience.
- The costs of current or proposed virtual desktop experiences need to be optimized to help organizations scale their remote work more effectively.
- The IT team wants to transform the workplace, which often starts with transforming employees' user experience.

Virtualization of your end users' desktops in the cloud can help your team realize each of these outcomes.

## Approach: Windows Virtual Desktop refactor and modernization

In the approach outlined in this article series, the existing Citrix, VMware, or Remote Desktop Services farms are modernized and replaced with a platform as a service (PaaS) solution called Windows Virtual Desktop.

In this scenario, desktop images are either migrated to Azure or new images are generated. Similarly, user profiles are either migrated to Azure or new profiles are created. For the most part, the client solution is enabled but largely unchanged by this migration effort.



When the migration to the cloud is finished, the overhead and costs of managing a virtual desktop farm are replaced with a cloud-native solution that manages the virtual desktop experience for your team. The team needs to be concerned only with support of the desktop images, available applications, Azure Active Directory, and user profiles.

## Next steps

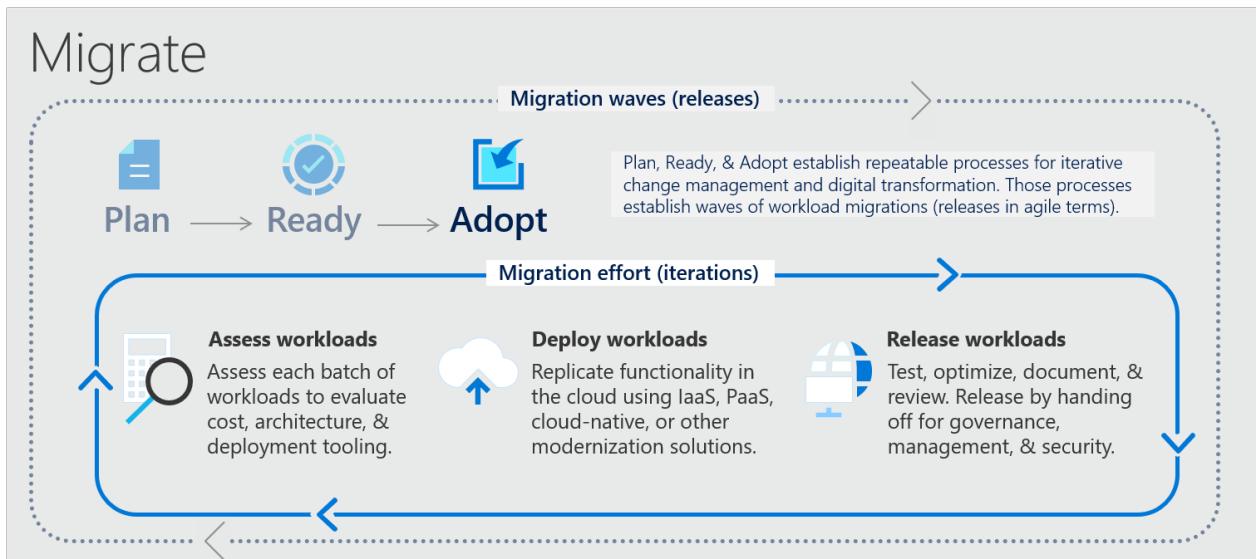
For guidance on specific elements of the cloud adoption journey, see:

- [Plan for Windows Virtual Desktop migration or deployment](#)
- [Review your environment or Azure landing zone\(s\)](#)
- [Complete a Windows Virtual Desktop proof-of-concept](#)
- [Assess for Windows Virtual Desktop migration or deployment](#)
- [Deploy or migrate Windows Virtual Desktop instances](#)
- [Release your Windows Virtual Desktop deployment to production](#)

# Windows Virtual Desktop planning

11/9/2020 • 2 minutes to read • [Edit Online](#)

Windows Virtual Desktop and deployment scenarios follow the same Migrate methodology as other migration efforts. This consistent approach allows migration factories or existing migration teams to adopt the process with little change to non-technical requirements.



## Plan your migration

As with other migrations, your team will assess workloads, deploy them, and then release them to end users. However, Windows Virtual Desktop includes specific requirements that will necessitate a review of the Azure landing zones during the assessment of the workloads. The process will also require a proof of concept prior to the first deployment.

To build your plan, see the [cloud adoption plan DevOps template](#) for an existing migration backlog in Azure DevOps. Use the template to create a detailed plan of activities.

## Next steps

For guidance on specific elements of the cloud adoption journey, see:

- [Review your environment or Azure landing zones](#)
- [Complete a Windows Virtual Desktop proof of concept](#)
- [Assess Windows Virtual Desktop migration or deployment](#)
- [Deploy or migrate Windows Virtual Desktop instances](#)
- [Release your Windows Virtual Desktop deployment to production](#)

# Windows Virtual Desktop Azure landing zone review

11/9/2020 • 2 minutes to read • [Edit Online](#)

Before the Contoso cloud adoption team migrates to Windows Virtual Desktop, it will need an Azure landing zone that's capable of hosting desktops and any supporting workloads. The following checklist can help the team evaluate the landing zone for compatibility. Guidance in the [Ready methodology](#) of this framework can help the team build a compatible Azure landing zone, if one has not been provided.

## Evaluate compatibility

- **Resource organization plan:** The landing zone should include references to the subscription or subscriptions to be used, guidance on resource group usage, and the tagging and naming standards to be used when the team deploys resources.
- **Azure AD:** An Azure Active Directory (Azure AD) instance or an Azure AD tenant should be provided for end-user authentication.
- **Network:** Any required network configuration should be established in the landing zone prior to migration.
- **VPN or ExpressRoute:** Additionally, any landing zone that supports virtual desktops will need a network connection so that end users can connect to the landing zone and hosted assets. If an existing set of endpoints is configured for virtual desktops, end users can still be routed through those on-premises devices via a VPN or Azure ExpressRoute connection. If a connection doesn't already exist, you might want to review the guidance on configuring network connectivity options in the [Ready methodology](#).
- **Governance, users, and identity:** For consistent enforcement, any requirements to govern access from virtual desktops and to govern users and their identities should be configured as Azure policies and applied to the landing zone.
- **Security:** The security team has reviewed the landing zone configurations and approved each landing zone for its intended use, including landing zones for the external connection and landing zones for any mission-critical applications or sensitive data.
- **Windows Virtual Desktop:** Windows Virtual Desktop platform as a service has been enabled.

Any landing zone that the team develops by using the best practices in the [Ready methodology](#) and that can meet the previously mentioned specialized requirements would qualify as a landing zone for this migration.

To understand how to architect Windows Virtual Desktop, review the [Windows Virtual Desktop requirements](#).

## Next steps

For guidance on specific elements of the cloud adoption journey, see:

- [Complete a Windows Virtual Desktop proof of concept](#)
- [Assess for Windows Virtual Desktop migration or deployment](#)
- [Deploy or migrate Windows Virtual Desktop instances](#)
- [Release your Windows Virtual Desktop deployment to production](#)

# Windows Virtual Desktop proof of concept

11/9/2020 • 2 minutes to read • [Edit Online](#)

Before the Contoso cloud adoption team deploys its end-user desktops, it validates the configuration of the Azure landing zone and end-user network capacity by completing and testing a proof of concept.

The following approach to the migration process is simplified to outline a proof-of-concept implementation.

1. **Assess:** the team deploys host pools by using the default virtual machine (VM) sizes. Assessment data helps the team identify the expected number of concurrent user sessions and the number of VMs required to support those concurrent sessions.
2. **Deploy:** the team [creates a host pool](#) for pooled desktops by using a Windows 10 gallery image from Azure Marketplace and the sizing from assessment step 1.
3. **Deploy:** the team [creates RemoteApp application groups](#) for workloads that it has already migrated.
4. **Deploy:** the team [creates an FSLogix profile container](#) to store user profiles.
5. **Release:** the team tests the performance and latency of application groups and deployed desktops for a sampling of users.
6. **Release:** the team onboards its end users to teach them how to connect through [Windows desktop client](#), [web client](#), [Android client](#), [macOS client](#), or [iOS client](#).

## Assumptions

The proof of concept approach could meet some production needs, but it's built on a number of assumptions.

It's unlikely that all the following assumptions will prove to be true for any enterprise migration of Windows Virtual Desktop. The adoption team should assume that the production deployment will require a separate deployment that more closely aligns to the production requirements that it identifies during the Windows Virtual Desktop assessment. The assumptions are:

- End users have a low-latency connection to the assigned landing zone in Azure.
- All users can work from a shared pool of desktops.
- All users can use the Windows 10 Enterprise multi-session image from Azure Marketplace.
- All user profiles will be migrated to either Azure Files, Azure NetApp Files, or a VM-based storage service for the FSLogix profile containers.
- All users can be described by a common persona with a density of six users per virtual central processing unit (vCPU) and 4 gigabytes (GB) of RAM, [as per the VM sizing recommendations](#).
- All workloads are compatible with Windows 10 multi-session.
- Latency between the virtual desktops and application groups is acceptable for production usage.

To calculate the cost of the Windows Virtual Desktop scenario based on the proof-of-concept configuration reference, the team uses the pricing calculator for [East US](#), [West Europe](#), or [Southeast Asia](#).

### NOTE

These examples all use Azure Files as the storage service for user profiles.

## Next steps

For guidance on specific elements of the cloud adoption journey, see:

- Assess for Windows Virtual Desktop migration or deployment
- Deploy or migrate Windows Virtual Desktop instances
- Release your Windows Virtual Desktop deployment to production

# Windows Virtual Desktop assessment

11/9/2020 • 5 minutes to read • [Edit Online](#)

The Windows Virtual Desktop [proof of concept](#) provides an initial scope as a baseline implementation for the Contoso cloud adoption team. But the output of that proof of concept is unlikely to meet their production needs.

The Windows Virtual Desktop assessment exercise serves as a focused means of testing assumptions through a data-driven process. Assessment data will help the team answer a series of important questions, validate or invalidate their assumptions, and refine the scope as necessary to support the team's Windows Virtual Desktop scenario. By using this assumption-validation approach, the team can accelerate the migration or deployment of its end-user desktops to Windows Virtual Desktop.

## Assess Windows Virtual Desktop deployments

Each Windows Virtual Desktop assessment will evaluate a combination of a user persona, a consistent host pool of virtual machines (VMs), end-user applications and data, and user profiles (data). During the assessment, the team's objective is to use data to answer the questions in this section. The answers will shape the actual scope of the deployment and release of the Windows Virtual Desktop migration.

The answers to these questions start with data. In the Plan methodology, specifically [best practices](#) and [digital estate assessment](#), data should already be collected and analyzed to create a migration plan. However, the questions in this specific workload assessment will likely require additional data. Data about the desktops, users, and workloads to be used by each user is required to develop a Windows Virtual Desktop deployment plan.

If you use [Movere](#) as your data collection tool, you'll likely have the data you need to develop personas and answer these questions by using data in [Azure Migrate](#), just like any other migration scenario.

If you don't have the data that you require to answer all the questions in this section, an additional third-party software vendor can provide a separate discovery process to augment the data you have. The vendor, [lakeside](#), is also integrated with Azure Migrate within the virtual desktop infrastructure migration goals section. The vendor can help you map out a plan for Windows Virtual Desktop deployment, including personas, host pools, applications, and user profiles.

### User personas

How many distinct personas will be required to support all of the users included in this migration scenario?

Defining personas will come as a result of bucketing users based on the following criteria:

- **Personal pools:** Do specific groups of users require dedicated desktops, instead of pools? For example, security, compliance, high-performance, or noisy-neighbor requirements might lead to some users running on dedicated desktops that aren't part of a pooling strategy. You'll enter this information by specifying a [host pool type of personal during the Windows Virtual Desktop host pool deployment](#).
- **Density:** Do specific groups of users require a lower-density desktop experience? For example, heavier density might require two users per virtual central processing unit (vCPU) instead of the light-user assumption of six users per vCPU. You'll enter density information in the [pool settings of the Windows Virtual Desktop host pool deployment](#).
- **Performance:** Do specific groups of users require a higher-performance desktop experience? For example, some users require more memory per vCPU than the assumed 4 gigabytes (GB) of RAM per vCPU. You'll enter the VM sizing in the [virtual machine details of the Windows Virtual Desktop host pool deployment](#).
- **Graphical processing (GPU):** Do specific groups of users have greater graphical requirements? For example, some users require GPU-based VMs in Azure, as demonstrated in this [guide for configuring GPU VMs](#).
- **Azure region:** Do specific groups of OS users operate from various geographic regions? For example, before

you configure the host pool, a user from each region should test latency to Azure by using the [estimation tool](#). The test user should share the lowest-latency Azure region and the latency in milliseconds for the top three Azure regions.

- **Business functions:** Can the specific groupings of users be bucketed by business unit, charge code, or their business function? This type of grouping will help align corporate costs in later stages of operations.
- **User count:** How many users will be in each distinct persona?
- **Max session counts:** Based on geography and hours of operation, how many concurrent users are expected for each persona during maximum load?

Distinctions in each of the preceding questions will start to illustrate user personas by business function, cost center, geographic region, and technical requirements. The following table can aid in recording responses to populate a completed assessment or design document:

CRITERION	PERSONA GROUP 1	PERSONA GROUP 2	PERSONA GROUP 3
Pools	Pools	Pools	Dedicated (security concerns)
Density	Light (6 users/vCPU)	Heavy (2 users/vCPU)	Dedicated (1 user/vCPU)
Performance	Low	High memory	Low
GPU	N/A	Required	N/A
Azure region	North America	Western Europe	North America
User count	1000	50	20
Session count	200	50	10

Each persona, or each group of users with distinct business functions and technical requirements, would require a specific host-pool configuration.

The end-user assessment provides the required data: pool type, density, size, CPU/GPU, landing zone region, and so on.

Host-pool configuration assessment now maps that data to a deployment plan. Aligning the technical requirements, business requirements, and cost will help determine the proper number and configuration of host pools.

See examples for pricing in the [East US](#), [West Europe](#), or [Southeast Asia](#) regions.

## Application groups

Both Movere and lakeside scans of the current on-premises environment can provide data about the applications that are run on end-user desktops. By using that data, you can create a list of all applications required per each persona. For each required application, the answers to the following questions will shape deployment iterations:

- Do any applications need to be installed for the persona to use this desktop? Unless the persona uses 100 percent web-based software as a service applications, you'll likely need to [configure a custom master VHD image](#) for each persona, with the required applications installed on the master image.
- Does this persona need Microsoft 365 applications? If so, you'll need to [add Microsoft 365 to a customized master VHD image](#).
- Is this application compatible with Windows 10 multi-session? If an application isn't compatible, a [personal pool](#) might be required to run the custom VHD image. For assistance with application and Windows Virtual

Desktop compatibility issues, see the [desktop application assure service](#).

- Are mission-critical applications likely to suffer from latency between the Windows Virtual Desktop instance and any back-end systems? If so, you might want to consider migrating the back-end systems that support the application to Azure.

The answers to these questions might require the plan to include remediation to the desktop images or supporting application components prior to desktop migration or deployment.

## Next steps

For guidance on specific elements of the cloud adoption journey, see:

- [Deploy or migrate Windows Virtual Desktop instances](#)
- [Release your Windows Virtual Desktop deployment to production](#)

# Windows Virtual Desktop deployment or migration

11/9/2020 • 4 minutes to read • [Edit Online](#)

The guidance in this article assumes that you've [established a plan for Windows Virtual Desktop](#), [assessed the desktop deployment requirements](#), [completed a proof of concept](#), and are now ready to migrate or deploy your Windows Virtual Desktop instances.

## Initial scope

The deployment of Windows Virtual Desktop instances follows a process that's similar to the [proof of concept](#) process. Use this initial scope as a baseline to explain the various scope changes that are required by the output of the assessment.

- [Create a host pool](#) for pooled desktops by using a Windows 10 gallery image from Azure Marketplace and the sizing from step 1 of that procedure.
- [Create RemoteApp application groups](#) for workloads that have already been migrated.
- [Create an FSLogix profile container](#) to store user profiles.

Deployment and migration consist of persona migration, application migration, and user profile migration. Depending on the results of the workload assessment, there will likely be changes to each of those migration tasks. This article helps identify ways that the scope would change based on the assessment feedback.

## Iterative methodology

Each persona will likely require an iteration of the previously outlined initial scope, resulting in multiple host pools. Depending on the Windows Virtual Desktop assessment, the adoption team should define iterations that are based on the number of personas or users per persona. Breaking the process into persona-driven iterations helps to reduce the change velocity impact on the business and allows the team to focus on proper testing or onboarding of each of the persona pools.

## Scope considerations

Each of the following sets of considerations should be included in the design documentation for each persona group to be migrated or deployed. After the scope considerations are factored in to the previously discussed [initial scope](#), the deployment or migration can begin.

### Azure landing zone considerations

Before you deploy the persona groups, a landing zone should be created in the Azure region that's required to support each persona to be deployed. Each assigned landing zone should be evaluated against the [landing zone review requirements](#).

If the assigned Azure landing zone doesn't meet your requirements, scope should be added for any modifications to be made to the environment.

### Application and desktop considerations

Some personas might have a dependency on legacy solutions, which are not compatible with Windows 10 multi-session. In these cases, some personas might require dedicated desktops. This dependency might not be discovered until deployment and testing.

If they're discovered late in the process, future iterations should be allocated to modernization or migration of the legacy application. This will reduce the long-term cost of the desktop experience. Those future iterations should be

prioritized and completed based on the overall pricing impact of modernization versus the extra cost associated with dedicated desktops. To avoid pipeline disruptions and the realization of business outcomes, this prioritization should not affect current iterations.

Some applications might require remediation, modernization, or migration to Azure to support the desired end-user experience. Those changes are likely to come after release. Alternately, when desktop latency can affect business functions, the application changes might create blocking dependencies for the migration of some personas.

### User profile considerations

The [initial scope](#) assumes that you're using a [VM-based FSLogix user profile container](#).

You can use [Azure NetApp Files to host user profiles](#). Doing so will require a few extra steps in the scope, including:

- **Per NetApp instance:** Configure NetApp files, volumes, and Active Directory connections.
- **Per host/persona:** Configure FSLogix on session host virtual machines.
- **Per user:** Assign users to the host session.

You can also use [Azure Files to host user profiles](#). Doing so will require a few extra steps in the scope, including:

- **Per Azure Files instance:** Configure the storage account, disk type, and Active Directory connection ([Active Directory Domain Services \(AD DS\) is also supported](#), assign role-based access control access for an Active Directory user group, apply new technology file system permissions, and get the storage account access key).
- **Per host/persona:** Configure FSLogix on session host virtual machines.
- **Per user:** Assign users to the host session.

The user profiles for some personas or users might also require a data migration effort, which can delay the migration of specific personas until user profiles can be remediated within your local Active Directory or individual user desktops. This delay could significantly affect the scope outside of the Windows Virtual Desktop scenario. After they've been remediated, the initial scope and the preceding approaches can be resumed.

## Deploy or migrate Windows Virtual Desktop

After all considerations are factored into your production scope for the Windows Virtual Desktop migration or deployment, the process can begin. On an iterative cadence, the adoption team will now deploy host pools, applications, and user profiles. After this phase is completed, the post deployment effort of [testing and onboarding users](#) can begin.

## Next steps

[Release your Windows Virtual Desktop deployment to production](#)

# Windows Virtual Desktop post-deployment

11/9/2020 • 2 minutes to read • [Edit Online](#)

The release process for the migration or deployment of Windows Virtual Desktop instances is relatively straightforward. This process mirrors the one that's used during the [Windows Virtual Desktop proof of concept](#):

- Test the performance and latency of application groups and deployed desktops for a sampling of users.
- Onboard end users to teach them how to connect via:
  - [Windows desktop client](#)
  - [Web client](#)
  - [Android client](#)
  - [macOS client](#)
  - [iOS client](#)

## Post-deployment

After the release has been completed, it's common to add [logging and diagnostics to better operate Windows Virtual Desktop](#). It's also common for operations teams to onboard the pooled hosts and desktop virtual machines into the [Azure server management best practices](#) to manage reporting, patching, and business continuity and disaster recovery configurations.

Although the release process is out of scope for this migration scenario, the process might expose the need to migrate additional workloads to Azure during subsequent iterations of migration. If you haven't configured Microsoft 365 or Azure Active Directory, your cloud adoption team might choose to onboard into those services upon the release of the desktop scenarios. For a hybrid operating model, operations teams might also choose to integrate Intune, System Center, or other configuration management tools to improve operations, compliance, and security.

## Next steps

After the Windows Virtual Desktop migration is complete, your cloud adoption team can begin the next scenario-specific migration. Alternately, if there are additional desktops to be migrated, you can reuse this article series to guide your next Windows Virtual Desktop migration or deployment.

- [Plan for Windows Virtual Desktop migration or deployment](#)
- [Review your environment or Azure landing zones](#)
- [Complete a Windows Virtual Desktop proof of concept](#)
- [Assess for Windows Virtual Desktop migration or deployment](#)
- [Deploy or migrate Windows Virtual Desktop instances](#)
- [Release your Windows Virtual Desktop deployment to production](#)

# SQL Server migration best practices for Azure

11/9/2020 • 2 minutes to read • [Edit Online](#)

Migrating SQL Server to Azure can accelerate the standard methodology outlined in the Cloud Adoption Framework. The process is shown in the following diagram.

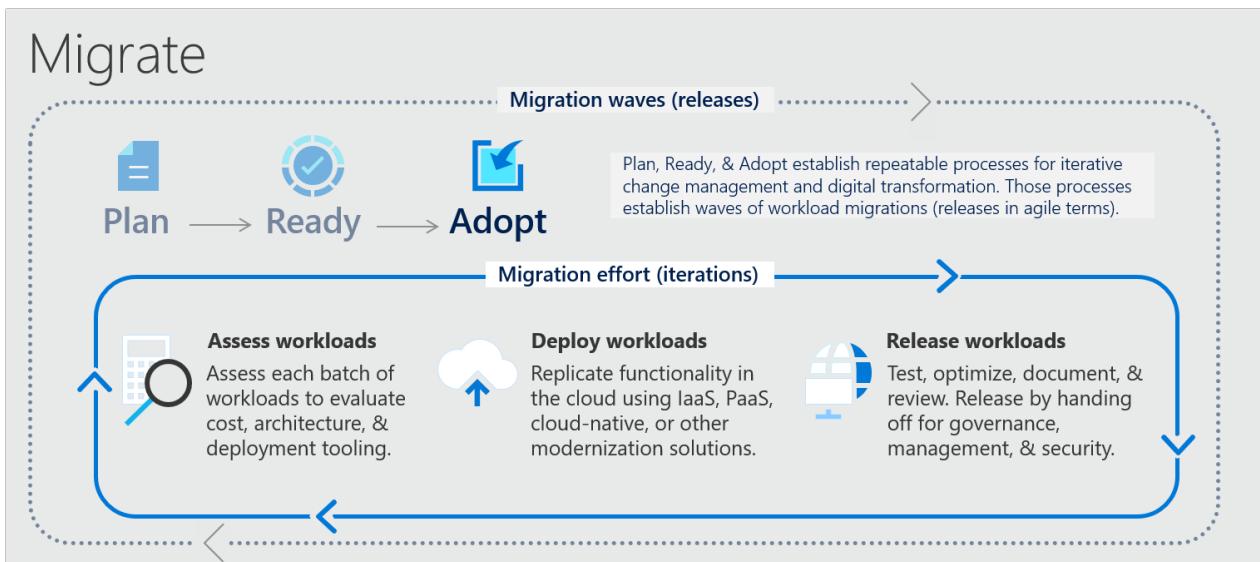


Figure 1

The table of contents on the left outlines best practices that can guide the execution of your SQL Server migration. You can migrate by using Azure Database Migration Guide, Azure Database Migration Service, or other tools. Bookmark this page for quick reference to the full list of best practices.

# Azure Stack: A strategic option for running Azure in your datacenter

11/9/2020 • 2 minutes to read • [Edit Online](#)

Microsoft takes a cloud-first approach to application and data storage. The priority is to move applications and data to one or more of the hyperscale clouds, including the global Azure option or a sovereign, locale-specific cloud such as Azure Germany or Azure Government.

Azure Stack Hub acts as another instance of a sovereign cloud, whether it's operated by customers in their datacenters or consumed through a cloud service provider. However, Azure Stack Hub is not a hyperscale cloud, and Microsoft doesn't publish or support any service-level agreements for Azure Stack Hub.

## Understand your cloud journey

Each organization has a unique journey to the cloud, depending on its history, business specifics, culture and, maybe most importantly, its starting point. Its journey provides many options, features, and functionalities. It also presents opportunities to improve its existing governance and operations, implement new ones, and even redesign its applications to take advantage of the cloud architectures.

Your organization's journey might identify clear benefits to using the cloud as part of your IT and business strategy. However, your journey could identify equally strong motivations to keep the cloud in your existing datacenter, at least for now. If you're facing these two competing drivers, you don't have to choose. At its core, Azure Stack Hub is [infrastructure as a service \(IaaS\)](#). It also provides platform as a service (PaaS) services that allow you to run a subset of Azure services in your own datacenter.

## Azure Stack Hub in your strategy

Azure Stack Hub provides an alternative approach to the migration of existing applications that run on either physical servers or existing virtualization platforms. By moving these workloads to an Azure Stack Hub IaaS environment, teams can benefit from smoother operations, self-service deployments, standardized hardware configurations, and Azure consistency. Using Azure Stack Hub for modernization or innovation support enables your teams to prepare your applications and workloads to take full advantage of the cloud.

By following a consistent practice for cloud adoption across Azure and Azure Stack Hub, you can apply the same governance and operations models to assets in the public cloud or your own datacenter. Azure Stack Hub uses the same Azure Resource Manager model as Azure, enabling that single-pane of glass view for your solutions.

## Compare Azure with Azure Stack Hub

There are some differences between Azure and Azure Stack Hub. Some are very visible, and others can't be seen until late in the implementation cycle. Be aware of the following differences:

- Azure offers near limitless capacity. Azure Stack Hub is built on physical hardware in your datacenter, which leads to capacity limitations.
- API versions and authentication mechanisms might be slightly different between Azure and Azure Stack Hub.
- Azure Stack Hub differs in *who* operates the cloud, which affects the level of workload operations.
- Consider which part of the Azure Stack Hub service the Azure Stack Hub operator runs on, because that determines whether the customer calls a service PaaS or software as a service (SaaS).

Other differences will be called out in other Azure Stack Hub articles at various points in the cloud adoption

lifecycle.

## Next steps

For guidance on specific elements of the cloud adoption journey, see:

- [Plan for Azure Stack Hub migration](#)
- [Environmental readiness](#)
- [Assess workloads for Azure Stack Hub](#)
- [Deploy workloads to Azure Stack Hub](#)
- [Govern Azure Stack Hub](#)
- [Manage Azure Stack Hub](#)

# Plan your Azure Stack Hub migration

11/9/2020 • 2 minutes to read • [Edit Online](#)

This article assumes that you've reviewed how to [integrate Azure Stack into your cloud strategy](#) and that your journey aligns with the examples in that article.

Before you move directly into your organization's migration efforts, it's important to set expectations appropriately about Azure and Azure Stack Hub. Doing so can help avoid pitfalls or setbacks later in the project. The key to a successful implementation is a good understanding of when to use Azure and when to use Azure Stack Hub.

## Digital estate alignment

Alignment of your organization's digital estate starts with a few simple questions to ask when you complete your [digital estate rationalization](#).

- What is the motivation, such as regulatory requirements, data gravity, or compliance needs, to keep applications and data on-premises?
- Which specific regulatory or compliance requirements affect the decision to stay in the datacenter?
- How will data privacy affect data migration?
- Is migration defined as a modernization journey?
- If so, have you defined the next steps and the goals required after the migration?
- What are the service-level agreement, recovery point objective, recovery time objective, and availability requirements?

For some workloads, your answers to these questions will fuel conversations about the value of Azure versus Azure Stack Hub for that workload.

## Assessment best practices

By applying the best practice for [assessing a digital estate with Azure Migrate](#), you can accelerate the assessment and alignment of the workloads and assets in your digital estate. This best practice provides insight into your full IT portfolio. It also helps identify technical requirements for capacity, scale, and configuration to guide your migration.

By using proper assessment data, your cloud adoption team can make wiser choices and establish clearer priorities when they evaluate options for public or private cloud platforms in Azure.

## Planning best practices

The following resources can help your team understand the differences between Azure and Azure Stack Hub:

- [Azure Stack overview and roadmap](#)
- [Azure Stack capacity planning](#)
- [Azure Stack Hub datacenter integration walkthrough](#)
- [Azure Stack virtual machine features](#)

When you understand the best platform for each workload, you can integrate your decisions into a [cloud adoption plan](#) to manage public and private cloud migrations as one aligned effort.

## Next steps

For guidance on specific elements of the cloud adoption journey, see:

- [Ready your cloud environment for Azure Stack Hub migration](#)
- [Assess workloads for Azure Stack Hub](#)
- [Deploy workloads to Azure Stack Hub](#)
- [Govern Azure Stack Hub](#)
- [Manage Azure Stack Hub](#)

# Ready your cloud environment for Azure Stack Hub migration

11/9/2020 • 2 minutes to read • [Edit Online](#)

This article assumes that you've decided to [integrate Azure Stack into your cloud strategy](#) and you've developed a [plan for Azure Stack Hub migration](#).

Assess the infrastructure dependencies that must be addressed first:

- Identity
- Connectivity
- Security
- Encryption

## Hybrid environment configuration

In a hybrid environment, some parts of your IT portfolio are in the Azure public cloud and others are in your Azure Stack Hub private cloud. To develop such an environment, you'll first want to configure a few basic elements in the public cloud. To begin establishing landing zones in the public cloud, see [Ensure that your environment is prepared for cloud adoption](#).

**Landing zone and cloud platform connections:** During the process, ensure that you have a stable network connection between your current datacenter and Azure. After you've established the network connection, test the latency, bandwidth, and reliability of the connection to Azure.

**Governance and operations:** When you migrate to both clouds, you need to make a few early decisions that will affect the environment. By applying best practices, you build on cloud-native operations and governance tools that run in the public cloud. This approach reduces the cost of running expensive systems in your datacenter or consuming capacity on your Azure Stack Hub. When you migrate to either form of the cloud, you need to either follow best practices or continue using existing systems for operations, governance, and change management.

## Private cloud environment

If you choose to only use the private cloud version of Azure, an Azure Stack Hub, you'll need to consider the same decision points:

**On-premises governance and operations:** The best practice still suggests using the cloud-native operations and governance tools found in the public cloud version of Azure. It's important to evaluate this best practice early and determine whether it's applicable to your scenario.

**Landing zone and cloud platform connections:** If your workload migrations will be deployed to your Azure Stack Hub, it will be important to document and test the latency, bandwidth, and reliability of the network routes between end users and your Azure Stack appliance.

## Next steps

For guidance on specific elements of the cloud adoption journey, see:

- [Assess workloads for Azure Stack Hub](#)
- [Deploy workloads to Azure Stack Hub](#)
- [Govern Azure Stack Hub](#)

- Manage Azure Stack Hub

# Assess workloads for Azure Stack Hub migration

11/9/2020 • 2 minutes to read • [Edit Online](#)

This article assumes that you've decided to [integrate Azure Stack into your cloud strategy](#), you've developed a [plan for Azure Stack Hub migration](#), and [your environment is ready for migration](#).

During the rationalization of your organization's digital estate in the Plan methodology, each workload was discovered and inventoried, and initial decisions were made based on quantitative data. Before you deploy each workload, it's important to validate the data and the decisions with qualitative data.

## Placement

The first data point to consider is placement. That is, will this workload be migrated to your public cloud, private cloud, or some other cloud platform, such as a sovereign cloud or service provider's Azure environment?

The information in each of the following sections can help validate your decisions about placement. The information will also help surface data that will be useful during the deployment of your workloads.

## Stakeholder value

Evaluate the value of migrating this workload with business and IT stakeholders:

- Less friction: short-term focus, limited long-term viability.
- More friction: long-term investment, easier to iterate and continue to modernize.
- A balance of the two.

## Governance, risk, and compliance

Assess the impact of regulatory, compliance, and privacy requirements:

- What data can reside on Azure and what data needs to stay on-premises?
- Who can manage the underlying platform?
- Is the data dependent on the location?
- Are there expiration dates for storing the data?

## Success metrics

Determine success metrics and availability tolerances:

- Performance
- Availability
- Resiliency
- Deployment or migration approach

## Licensing

Assess the impact of licensing and support:

- Are there product licensing restrictions that will limit transformation?
- Is the application or dataset supportable in the new environment?
- Are there third-party software vendors who need to provide support statements?

## Operations requirements

- Avoid duplication of effort and optimize service-level agreements (SLAs) by examining the correlation between IT-managed cloud services and application-specific services.
- Consider the automation that's required to orchestrate the provisioning of services during deployment and migration of applications.
- To help meet your operations requirements, consider [scalability and availability](#) services such as pay per use, virtual machine (VM) availability sets, VM scale sets, network adapters, and the ability to add and resize VMs and disks.

## Monitoring

- Monitor system health and operational status and performance by using well-defined metrics that form the basis of the SLAs that you offer your end users.
- Check security and compliance, evaluating how well the cloud environment meets the regulatory and compliance requirements that are imposed by the application.
- What are the processes for backup/restore and replication/failover?
- Find data-protection services for infrastructure as a service, platform as a service, and software as a service resources.
- Incorporate multiple vendors, technologies, and capabilities to achieve a comprehensive protection strategy.

## Next steps

For guidance on specific elements of the cloud adoption journey, see:

- [Assess workloads for Azure Stack Hub](#)
- [Deploy workloads to Azure Stack Hub](#)
- [Govern Azure Stack Hub](#)
- [Manage Azure Stack Hub](#)

# Deploy workloads to Azure Stack Hub

11/9/2020 • 2 minutes to read • [Edit Online](#)

By using Azure Stack, your organization can run its own instance of Azure in its datacenter. Organizations include Azure Stack in their cloud strategy because it helps them handle situations when the public cloud won't work for them. The three most common reasons to use Azure Stack are:

- Poor network connectivity to the public cloud.
- Regulatory or contractual requirements.
- Back-end systems that can't be exposed to the internet.

## Infrastructure as a service deployment

Regardless of the reason to deploy infrastructure as a service (IaaS), deployment to Azure Stack Hub is similar to any other IaaS deployment. People often think of IaaS only as virtual machines (VMs), but IaaS is more than that. When you deploy a VM in Azure or Azure Stack, the machine comes with a software-defined network, including domain name system, public IPs, firewall rules (also called network security groups), and many other capabilities. The VM deployment also creates disks for your VMs on software-defined storage by using Azure Blob storage.

For deeper guidance on deploying VMs to Azure Stack, see the [Azure Stack compute overview](#).

## Platform as a service deployment

In the cloud, all platform as a service (PaaS) resources run on some form of infrastructure service, such as a VM. However, Azure services obfuscate those backend resources so you don't have to manage them. The obfuscation and coordination of those infrastructure resources is managed by Azure Resource Manager. You may have seen one aspect of Resource Manager when deploying to Azure using an Azure Resource Manager template. Those templates tell Azure which resource provider you want to invoke and how you want your resources to be configured.

When the cloud runs in your datacenter, your stack hub administrators will need to be somewhat familiar with the layers of obfuscation. Before your users or developers can use a PaaS resource, the Azure Stack Hub administrator will need to install the resource provider from the marketplace. Those resource providers allow your instance of Azure Stack Hub to replicate the resource provider functionality of Azure in your stack instance. For more information on deploying Azure Stack Hub resource providers, see the [Azure Stack IaaS blog series](#).

## Deploy workloads

After the Azure Stack Hub administrator has properly configured your stack instance, migrations can continue as they would with most other Azure migration efforts. By using Azure Stack, your team can run any of the following types of migration:

- [Ethereum blockchain network](#)
- [AKS engine](#)
- [Azure Cognitive Services](#)
- [C# ASP.NET web app](#)
- [Linux VM](#)
- [Java web app](#)

## Additional considerations during migration

The following articles can help your team during migration and modernization:

- [Scalability and availability](#) services such as pay per use, VM availability sets, VM scale sets, network adapters, and the ability to add and resize VMs and disks
- [Storage capacity](#), including the ability to upload and download and also capture and deploy VM images
- [Azure Stack quickstart templates](#) GitHub repository
- [Azure quickstart templates](#) GitHub repository

## Next steps

For guidance on specific elements of the cloud adoption journey, see:

- [Govern Azure Stack Hub](#)
- [Manage Azure Stack Hub](#)

# Govern an Azure instance in your datacenter

11/9/2020 • 2 minutes to read • [Edit Online](#)

Governing hybrid solutions across public and private cloud platforms adds complexity. Because your Azure Stack Hub is your own private instance of Azure running in your datacenter, that complexity is inherently reduced.

The business processes, disciplines, and many of the best practices outlined in the [Govern methodology](#) of the Cloud Adoption Framework can still be applied to hybrid governance with Azure Stack Hub. Many cloud-native tools used in the public cloud version of Azure can also be used in your Azure Stack Hub.

## Azure Stack Hub governance considerations

The following series of blogs shows how your organization can implement cloud governance concepts for Azure Stack Hub:

- [Organizational services](#) such as resource groups, role-based access control (RBAC), change auditing, locks, and tags.
- [Security services](#), including default firewalls, restrictions, VM updates and patch management, and malware status.
- [DevOps options](#), including infrastructure as code, a portal with PowerShell and command-line interface, Azure Application Insights, and integration with Azure DevOps and Jenkins.

## Governance toolchain for Azure Stack Hub

For guidance on applying cloud-native governance tools to Azure Stack Hub environments, see:

- [Azure Resource Manager templates and Desired State Configuration](#)
- [PowerShell](#)
- [Azure Policy](#)
- [Role-based access control](#)

## Next steps

For guidance on specific elements of the cloud adoption journey, see:

- [Manage Azure Stack Hub](#)

# Manage workloads that run on Azure Stack Hub

11/9/2020 • 2 minutes to read • [Edit Online](#)

Operations and management of hybrid solutions across public and private cloud platforms is complex and could introduce risk to business operations. Because Azure Stack Hub is your organization's private instance of Azure running in your datacenter, the risk of hybrid operations is greatly reduced.

As outlined in the [Manage methodology](#) of the Cloud Adoption Framework, suggested operations management activities focus on the following list of core responsibilities. The same responsibilities hold true for the operations management teams that support Azure Stack Hub.

- **Inventory and visibility:** Create an inventory of assets across multiple clouds. Develop visibility into the run state of each asset.
- **Operational compliance:** Establish controls and processes to ensure that each state is properly configured and running in a well-governed environment.
- **Protect and recover:** Ensure that all managed assets are protected and can be recovered by using baseline management tooling.
- **Enhanced baseline options:** Evaluate common additions to the baseline that might meet business needs.
- **Platform operations:** Extend the management baseline with a well-defined service catalog and centrally managed platforms.
- **Workload operations:** Extend the management baseline to include a focus on mission-critical workloads.

## Considerations for Azure Stack Hub operations management

Some of the standard operations management activities require slightly different technical considerations. The following articles outline those considerations.

- [Self-service support](#) for your customers, including boot diagnostics, screenshots, serial logs, and metrics.
- [Guest management](#), including virtual machine (VM) extensions, the ability to run custom code, software inventory, and change tracking.
- [Business continuity](#) through VM backups and disaster recovery options.

## Next steps

After your Azure Stack Hub migration reaches an operational state, you can begin the next iteration of migrations by using Azure Stack Hub or other migration scenarios in the Azure public cloud.

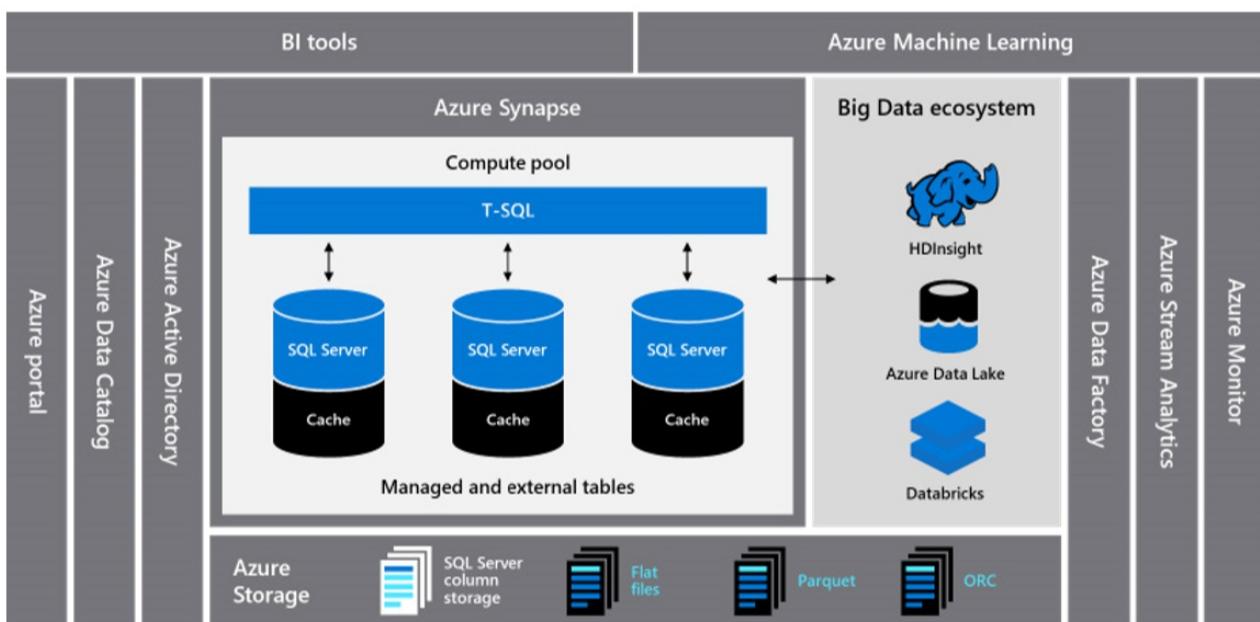
- [Plan for Azure Stack Hub migrations](#)
- [Environmental readiness](#)
- [Assess workloads for Azure Stack Hub](#)
- [Deploy workloads to Azure Stack Hub](#)
- [Govern Azure Stack Hub](#)
- [Manage Azure Stack Hub](#)

# Azure Synapse Analytics solutions

11/9/2020 • 2 minutes to read • [Edit Online](#)

Current market offerings fall short in meeting an organization's growing needs. Legacy on-premises environments, including Teradata, Netezza, and Oracle Exadata, are expensive, slow to innovate, and inelastic. Organizations that use on-premises systems are now considering taking advantage of innovative cloud, infrastructure as a service, and platform as a service offerings in newer environments like Azure.

Many organizations are ready to take the step of shifting expensive tasks like infrastructure maintenance and platform development to a cloud provider. In Microsoft Azure, an organization has access to a globally available, highly secure, scalable cloud environment that includes Azure Synapse Analytics in an ecosystem of supporting tools and capabilities.



Azure Synapse Analytics provides best-of-class relational database performance through techniques like massively parallel processing and automatic in-memory caching. The results of this approach can be seen in independent benchmarks like the one run recently by [GigaOm](#), which compares Azure Synapse to other popular cloud data warehouse offerings.

Organizations that have already migrated to Azure Synapse Analytics have seen many benefits, including:

- Improved performance and price for performance.
- Increased agility and shorter time to value.
- Faster server deployment and application development.
- Elastic scalability to ensure that you pay only for what you use.
- Improved security and compliance.
- Reduced storage and disaster recovery costs.
- Lower overall TCO and better cost control (operating expenses).

To maximize these benefits, it's necessary to migrate existing data and applications to the Azure Synapse platform. In many organizations, this approach includes migrating an existing data warehouse from a legacy on-premises platform like Teradata, Netezza, or Exadata. Organizations need to modernize their data estate with an analytics offering that is price-performant, rapidly innovative, scalable, and truly elastic. Learn more in the following sections for migration best practices on Teradata, Netezza, and Exadata.

## Next steps

- [Azure Synapse Analytics solutions for Teradata](#)
- [Azure Synapse Analytics solutions for Netezza](#)
- [Azure Synapse Analytics solutions for Exadata](#)

# Azure Synapse Analytics solutions and migration for Teradata

11/9/2020 • 18 minutes to read • [Edit Online](#)

Many organizations are ready to take the step of shifting expensive data warehouse tasks like infrastructure maintenance and platform development to a cloud provider. Organizations are now looking to take advantage of innovative cloud, infrastructure as a service, and platform as a service offerings in newer environments like Azure.

Azure Synapse Analytics is a limitless analytics service that brings together enterprise data warehousing and big data analytics. It gives you the freedom to query data on your terms at scale by using either serverless on-demand or provisioned resources. Learn what to plan for as you migrate a legacy Teradata system to Azure Synapse.

Although Teradata and Azure Synapse are similar in that they're both SQL databases that are designed to use massively parallel processing techniques to achieve high query performance on large data volumes, they have some basic differences:

- Legacy Teradata systems are installed on-premises, and they use proprietary hardware. Azure Synapse is cloud-based and uses Azure compute and storage resources.
- Upgrading a Teradata configuration is a major task that involves extra physical hardware and a potentially lengthy database reconfiguration or dump and reload. In Azure Synapse, compute and storage resources are separate, so you can easily scale up or down independently by using the elastic scalability of Azure.
- Without a physical system to support, you can pause or resize Azure Synapse as needed to reduce resource utilization and cost. In Azure, you have access to a globally available, highly secure, and scalable cloud environment that includes Azure Synapse in an ecosystem of supporting tools and capabilities.

In this article, we look at schema migration, with an objective of obtaining equivalent or increased performance of your migrated Teradata data warehouse and data marts on Azure Synapse. We consider concerns that apply specifically to migrating from an existing Teradata environment.

At a high level, the migration process includes the steps that are listed in the following table:

PREPARATION	MIGRATION	POST-MIGRATION
<ul style="list-style-type: none"><li>• Define scope: what do we want to migrate?</li><li>• Build an inventory of data and processes to migrate.</li><li>• Define any data model changes.</li><li>• Identify the best Azure and third-party tools and features to use.</li><li>• Train staff early on the new platform.</li><li>• Set up the Azure target platform.</li></ul>	<ul style="list-style-type: none"><li>• Start small and simple.</li><li>• Automate where possible.</li><li>• Use Azure built-in tools and features to reduce the migration effort.</li><li>• Migrate metadata for tables and views.</li><li>• Migrate relevant historical data.</li><li>• Migrate or refactor stored procedures and business processes.</li><li>• Migrate or refactor ETL/ELT incremental load processes.</li></ul>	<ul style="list-style-type: none"><li>• Monitor and document all stages of the migration process.</li><li>• Use experience gained to build a template for future migrations.</li><li>• Reengineer the data model if necessary by using the new platform's performance and scalability.</li><li>• Test applications and query tools.</li><li>• Benchmark and optimize query performance.</li></ul>

When you migrate from a legacy Teradata environment to Azure Synapse, in addition to the more general subjects that are described in the Teradata documentation, you must consider some specific factors.

## Initial migration workload

Legacy Teradata environments typically evolve over time to encompass multiple subject areas and mixed workloads. When you're deciding where to start on an initial migration project, it makes sense to choose an area that:

- Proves the viability of migrating to Azure Synapse by quickly delivering the benefits of the new environment.
- Allows in-house technical staff to gain experience with new processes and tools so that they can use them to migrate other areas.
- Creates a template based on the current tools and processes to use in additional migration from the source Teradata environment.

A good candidate for an initial migration from a Teradata environment that would support these objectives usually is one that implements a Power BI/analytics workload rather than an OLTP workload. The workload should have a data model that can be migrated with minimal modifications, such as a star or snowflake schema.

For size, it's important that the data volume you migrate in the initial exercise is large enough to demonstrate the capabilities and benefits of the Azure Synapse environment with a short time to demonstrate value. The size that typically meets the requirements is in the range of 1 to 10 terabytes (TB).

An approach for the initial migration project that minimizes risk and implementation time is to confine the scope of the migration to data marts. In Teradata, a good example is the OLAP database part of a Teradata data warehouse. This approach is a good starting point because it limits the scope of the migration, and it often can be achieved on a short timescale.

An initial migration scope of data marts only doesn't address broader concerns like how to migrate ETL and historical data. You must address these areas in later phases and backfill the migrated data mart layer with the data and processes that are required to build them.

## Lift-and-shift approach vs. phased approach

Regardless of the drivers and scope you choose for your migration, you can choose from two general types of migrations:

- **Lift-and-shift approach:** In this approach, the existing data model, such as a star schema, is migrated unchanged to the new Azure Synapse platform. The emphasis is on minimizing risk and the time it takes to migrate by reducing the work that's required to achieve the benefits of moving to the Azure cloud environment.

This approach is a good fit for existing Teradata environments in which a single data mart is to be migrated and if the data is already in a well-designed star or snowflake schema. This approach is a good choice also if you have time and cost pressures to move to a more modern cloud environment.

- **Phased approach that incorporates modifications:** If your legacy warehouse has evolved over time, you might need to reengineer the data warehouse to maintain the required performance or to support new data sources like IoT streams. Migrating to Azure Synapse for the well-known benefits of a scalable cloud environment might be considered part of the reengineering process. This process might include changing the underlying data model, such as moving from an Inmon model to Azure Data Vault.

The approach we recommend is to initially move the existing data model as-is to Azure. Then, take advantage of the performance and flexibility of Azure services to apply the reengineering changes without affecting the existing source system.

## Virtual machine colocation to support migration

An optional approach to migrate from an on-premises Teradata environment takes advantage of inexpensive cloud storage and elastic scalability in Azure. First, you create a Teradata instance on an Azure virtual machine that's colocated with the target Azure Synapse environment. Then, you use a standard Teradata utility like Teradata

Parallel Transporter or a third-party data replication tool like Qlik Replicate (formerly by Attunity) to efficiently move the subset of Teradata tables that you're migrating to the VM instance. All migration tasks take place in the Azure environment.

This approach has several benefits:

- After the initial replication of data, the source system isn't affected by other migration tasks.
- Familiar Teradata interfaces, tools, and utilities are available in the Azure environment.
- After the migration shifts to the Azure environment, you don't have any potential issues with network bandwidth availability between the on-premises source system and the cloud target system.
- Tools like Azure Data Factory efficiently call utilities like Teradata Parallel Transporter to migrate data quickly and easily.
- The migration process is orchestrated and controlled entirely from within the Azure environment.

## Metadata migration

It makes sense to automate and orchestrate the migration process by using the capabilities of the Azure environment. This approach minimizes impact on the existing Teradata environment, which might already be running close to full capacity.

Azure Data Factory is a cloud-based data integration service. You can use Data Factory to create data-driven workflows in the cloud to orchestrate and automate data movement and data transformation. Data Factory pipelines can ingest data from disparate datastores. Then, they process and transform the data by using compute services like Azure HDInsight for Apache Hadoop and Apache Spark, Azure Data Lake Analytics, and Azure Machine Learning.

Start by creating metadata that lists the data tables you want to migrate along with their locations. Then, use Data Factory capabilities to manage the migration process.

## Design differences between Teradata and Azure Synapse

As you plan your migration from a legacy Teradata environment to Azure Synapse, it's important to consider the design differences between the two platforms.

### Multiple databases vs. a single database and schemas

In a Teradata environment, you might have multiple, separate databases for different parts of the overall environment. For example, you might have a separate database for data ingestion and staging tables, a database for core warehouse tables, and another database for data marts (sometimes called a *semantic layer*). Processing separate databases as ETL/ELT pipelines in Azure Synapse might require implementing cross-database joins and moving data between the separate databases.

The Azure Synapse environment has a single database. Schemas are used to separate tables into logically separate groups. We recommend that you use a series of schemas in Azure Synapse to mimic any separate databases you migrate from Teradata.

If you use schemas in the Teradata environment, you might need to use a new naming convention to move the existing Teradata tables and views to the new environment. For example, you might concatenate the existing Teradata schema and table names into the new Azure Synapse table name, and then use schema names in the new environment to maintain the original separate database names.

Another option is to use SQL views over the underlying tables to maintain their logical structures. There are some potential downsides to using SQL views:

- Views in Azure Synapse are read-only, so you must make any updates to the data on the underlying base tables.
- If layers of views already exist, adding another layer of views might affect performance.

## Tables

When you migrate tables between different technologies, you physically move only raw data and the metadata that describes it between the two environments. You don't migrate database elements like indexes from the source system because they might not be needed, or they might be implemented differently in the new environment.

However, understanding where performance optimizations like indexes have been used in the source environment can be a helpful indication of where you might optimize performance in the new environment. For example, if a non-unique secondary index was created in the source Teradata environment, you might conclude that it would be advantageous to create a nonclustered index in the migrated Azure Synapse environment, or that using other native performance optimization techniques like table replication might be preferable to creating a like-for-like index.

## High availability database

Teradata supports data replication across nodes via the `FALLBACK` option. Table rows that reside physically on a node are replicated to another node within the system. This approach guarantees that data isn't lost if a node fails, and it provides the basis for failover scenarios.

The goal of the high-availability architecture in Azure SQL Database is to guarantee that your database is up and running 99.99% of the time. You don't need to consider how maintenance operations and outages might affect your workload. Azure automatically handles critical servicing tasks like patching, backups, and Windows and SQL upgrades, and unplanned events like underlying hardware, software, or network failures.

Snapshots are a built-in feature of the service that creates restore points in Azure Synapse. Snapshots provide automatic backup for data storage in Azure Synapse. You don't have to enable the capability. Currently, individual users can't delete automatic restore points that the service uses to maintain SLAs for recovery.

Azure Synapse takes snapshots of the data warehouse throughout the day. The restore points that it creates are available for seven days. The retention period can't be changed. Azure Synapse supports an eight-hour recovery point objective. You can restore your data warehouse in the primary region from any of the snapshots taken in the past seven days. Other user-defined options are available if your organization needs more granular backups.

## Unsupported Teradata table types

Teradata includes support for special table types for time series and temporal data. Azure Synapse doesn't directly support the syntax and some of the functions for these table types, but you can migrate the data into a standard table that has the required data types and indexing or partitioning on the date/time column.

Teradata implements temporal query functionality by using query rewriting to add filters to a temporal query to limit the applicable date range. If you use temporal queries in the source Teradata environment and you want to migrate it, you must add filters to the relevant temporal queries.

The Azure environment also includes features for complex analytics on time series data at scale through Azure Time Series Insights. Time Series Insights is designed for IoT data analysis applications, and it might be more appropriate for that use case. For more information, see [Azure Time Series Insights](#).

## Teradata data type mapping

Some Teradata data types aren't directly supported in Azure Synapse. The following table shows these data types and the recommended approach for handling them. In the table, the Teradata column type is the type that's stored in the system catalog (for example, in `DBC.ColumnsV`).

Use the metadata from the Teradata catalog tables to determine whether any of these data types should be migrated, and then plan for supporting resources in your migration plan. For example, you can use a SQL query like the one in the next section to find any occurrences of unsupported data types that you need to address.

Third-party vendors offer tools and services that can automate migration, including mapping data types between platforms. If you already use a third-party ETL tool like Informatica or Talend in the Teradata environment, you can use the tool to implement any required data transformations.

# SQL Data Manipulation Language (DML) syntax differences

You should be aware of a few differences in SQL Data Manipulation Language (DML) syntax between Teradata SQL and Azure Synapse:

- **QUALIFY**: Teradata supports the **QUALIFY** operator.

For example:

```
SELECT col1 FROM tab1 WHERE col1='XYZ'
```

Third-party tools and services can automate data-mapping tasks:

```
QUALIFY ROW_NUMBER() OVER (PARTITION by col1 ORDER BY col1) = 1;
```

In Azure Synapse, you can achieve the same result by using the following syntax:

```
SELECT * FROM (SELECT col1, ROW_NUMBER() OVER (PARTITION by col1 ORDER BY col1) rn FROM tab1 WHERE c1='XYZ' ) WHERE rn = 1;
```

- **Date arithmetic**: Azure Synapse has operators like **DATEADD** and **DATEDIFF**, which you can use on **DATE** or **DATETIME**.

Teradata supports direct subtraction on dates:

- `SELECT DATE1 - DATE2 FROM ...`
- `LIKE ANY` syntax

Example:

```
SELECT * FROM CUSTOMER WHERE POSTCODE LIKE ANY ('CV1%', 'CV2%', CV3%') .
```

The equivalent in Azure Synapse syntax is:

```
SELECT * FROM CUSTOMER WHERE (POSTCODE LIKE 'CV1%') OR (POSTCODE LIKE 'CV2%') OR (POSTCODE LIKE 'CV3%') ;
```

- Depending on system settings, character comparisons in Teradata might not be case-specific by default. In Azure Synapse, these comparisons are always case-specific.

## Functions, stored procedures, triggers, and sequences

When you migrate a data warehouse from a mature legacy environment like Teradata, often you need to migrate elements other than simple tables and views to the new target environment. Examples of non-table elements in Teradata that you might need to migrate to Azure Synapse are functions, stored procedures, triggers, and sequences. During the preparation phase of the migration, you should create an inventory of objects to migrate. In the project plan, define the method of handling all objects and allocate the appropriate resources to migrate them.

You might find services in the Azure environment that replace the functionality implemented as functions or stored procedures in the Teradata environment. Usually, it's more efficient to use the built-in Azure capabilities instead of recoding the Teradata functions.

Here's more information about migrating functions, stored procedures, triggers, and sequences:

- **Functions**: Like most database products, Teradata supports system functions and user-defined functions in a SQL implementation. When common system functions are migrated to another database platform like Azure Synapse, they're usually available in the new environment and can be migrated without change. If system functions have slightly different syntax in the new environment, you usually can automate the required changes.

You might need to recode arbitrary user-defined functions and system functions that have no equivalent in

the new environment. Use the languages that are available in the new environment. Azure Synapse uses the popular Transact-SQL language to implement user-defined functions.

- **Stored procedures:** In most modern database products, you can store procedures in the database. A stored procedure typically contains SQL statements and some procedural logic. It might also return data or a status.

Teradata provides stored procedure language to create stored procedures. Azure Synapse supports stored procedures by using T-SQL. If you migrate stored procedures to Azure Synapse, you must recode them by using T-SQL.

- **Triggers:** You can't create triggers in Azure Synapse, but you can implement triggers in Data Factory.
- **Sequences:** Azure Synapse sequences are handled similarly to how they are handled in Teradata. Use `IDENTITY` columns or SQL code to create the next sequence number in a series.

## Metadata and data extraction

Consider the following information when you plan how to extract metadata and data from the Teradata environment:

- **Data Definition Language (DDL) generation:** As described earlier, it's possible to edit existing Teradata `CREATE TABLE` and `CREATE VIEW` scripts to create the equivalent definitions, with modified data types, if necessary. In this scenario, you usually must remove extra Teradata-specific clauses (for example, `FALLBACK`).

The information that specifies the current table and view definitions is maintained in system catalog tables. System catalog tables are the best source of the information because the tables likely are up to date and complete. User-maintained documentation might not be in sync with current table definitions.

You can access the information by using views on the catalog, such as `DBC.ColumnsV`. You also can use views to generate the equivalent `CREATE TABLE` Data Definition Language (DDL) statements for the equivalent tables in Azure Synapse.

Third-party migration and ETL tools also use the catalog information to achieve the same result.

- **Data extraction**

Migrate the raw data from existing Teradata tables by using standard Teradata utilities like `BTEQ` and `FASTEXPORT`. In a migration exercise, it's generally important to extract the data as efficiently as possible. The approach we recommend for recent versions of Teradata is to use Teradata Parallel Transporter, a utility that uses multiple parallel `FASTEXPORT` streams to achieve the best throughput.

You can call Teradata Parallel Transporter directly from Data Factory. We recommend this approach for managing the data migration process, whether the Teradata instance is on-premises or copied to a VM in the Azure environment, as described earlier.

The data formats we recommend for extracted data are delimited text files (also called *comma-separated values*), optimized row columnar files, or Parquet files.

For detailed information about the process of migrating data and ETL from a Teradata environment, see the Teradata documentation.

## Performance-tuning recommendations

The platforms have some differences when it comes to optimization. In the following list of performance-tuning recommendations, lower-level implementation differences between Teradata and Azure Synapse and alternatives for your migration are highlighted:

- **Data distribution options:** In Azure, you can set the data distribution methods for individual tables. The

purpose of the functionality is to reduce the amount of data that moves between processing nodes when a query is executed.

For large table/large table joins, hash distributing in one or both (ideally, both) tables on the join columns helps ensure that join processing can be performed locally because the data rows to be joined are already colocated on the same processing node.

Azure Synapse provides an additional way to achieve local joins for small table/large table joins (often called a *dimension table/fact table join* in a star schema model). You replicate the smaller table across all nodes, thereby ensuring that any value of the join key for the larger table has a matching dimension row that's locally available. The overhead of replicating the dimension table is relatively low if the tables aren't large. In this case, using the hash distribution approach described earlier is preferable.

- **Data indexing:** Azure Synapse provides various indexing options, but the options are different in operation and usage from indexing options in Teradata. To learn about the indexing options in Azure Synapse, see [Design tables in an Azure Synapse pool](#).

Existing indexes in the source Teradata environment can provide a useful indication of how data is used and provide an indication of candidate columns for indexing in the Azure Synapse environment.

- **Data partitioning:** In an enterprise data warehouse, fact tables might contain many billions of rows of data. Partitioning is a way to optimize maintenance and querying in these tables. Splitting the tables into separate parts reduces the amount of data processed at one time. Partitioning for a table is defined in the `CREATE TABLE` statement.

Only one field per table can be used for partitioning. The field that's used for partitioning frequently is a date field because many queries are filtered by date or by a date range. You can change the partitioning of a table after initial load. To change a table's partitioning, re-create the table with a new distribution that uses the `CREATE TABLE AS SELECT` statement. For a detailed description of partitioning in Azure Synapse, see [Partition tables in an Azure Synapse SQL pool](#).

- **Data table statistics:** You can ensure that statistics about data tables are up to date by adding a `COLLECT STATISTICS` step in ETL/ELT jobs or by enabling automatic statistics collection on the table.
- **PolyBase for data loading:** PolyBase is the most efficient method to use to load large amounts of data into a warehouse. You can use PolyBase to load data in parallel streams.
- **Resource classes for workload management:** Azure Synapse uses resource classes to manage workloads. In general, large resource classes provide better individual query performance. Smaller resource classes give you higher levels of concurrency. You can use dynamic management views to monitor utilization to help ensure that the appropriate resources are used efficiently.

## Next steps

For more information about implementing a Teradata migration, talk with your Microsoft account representative about on-premises migration offers.

# Azure Synapse Analytics solutions and migration for Netezza

11/9/2020 • 17 minutes to read • [Edit Online](#)

As IBM support for Netezza ends, many organizations that currently use Netezza data warehouse systems are looking to take advantage of innovative cloud, infrastructure as a service, and platform as a service offerings in newer environments like Azure. Many organizations are ready to take the step of shifting expensive tasks like infrastructure maintenance and platform development to a cloud provider.

Azure Synapse Analytics is a limitless analytics service that brings together enterprise data warehousing and big data analytics. It gives you the freedom to query data on your terms at scale by using either serverless on-demand or provisioned resources. Learn what to plan for as you migrate a legacy Netezza system to Azure Synapse.

Netezza and Azure Synapse are similar in that each is a SQL database that's designed to use massively parallel processing techniques to achieve high query performance on large data volumes. But the two platforms are different in key aspects:

- Legacy Netezza systems are installed on-premises, and they use proprietary hardware. Azure Synapse is cloud-based and uses Azure compute and storage resources.
- Upgrading a Netezza configuration is a major task that involves extra physical hardware and a potentially lengthy database reconfiguration or dump and reload. In Azure Synapse, storage and compute resources are separate. You can use the elastic scalability of Azure to independently scale up or down.
- Without a physical system to support, you can pause or resize Azure Synapse as needed to reduce resource utilization and cost. In Azure, you have access to a globally available, highly secure, and scalable cloud environment that includes Azure Synapse in an ecosystem of supporting tools and capabilities.

In this article, we look at schema migration, with a view to obtaining equivalent or increased performance of your migrated Netezza data warehouse and data marts on Azure Synapse. We consider concerns that apply specifically to migrating from an existing Netezza environment.

At a high level, the migration process includes the steps that are listed in the following table:

PREPARATION	MIGRATION	POST-MIGRATION
<ul style="list-style-type: none"><li>• Define scope: what do we want to migrate?</li><li>• Build an inventory of data and processes to migrate.</li><li>• Define any data model changes.</li><li>• Identify the best Azure and third-party tools and features to use.</li><li>• Train staff early on the new platform.</li><li>• Set up the Azure target platform.</li></ul>	<ul style="list-style-type: none"><li>• Start small and simple.</li><li>• Automate where possible.</li><li>• Use Azure built-in tools and features to reduce the migration effort.</li><li>• Migrate metadata for tables and views.</li><li>• Migrate relevant historical data.</li><li>• Migrate or refactor stored procedures and business processes.</li><li>• Migrate or refactor ETL or ELT incremental load processes.</li></ul>	<ul style="list-style-type: none"><li>• Monitor and document all stages of the migration process.</li><li>• Use experience gained to build a template for future migrations.</li><li>• Reengineer the data model if necessary by using the new platform's performance and scalability.</li><li>• Test applications and query tools.</li><li>• Benchmark and optimize query performance.</li></ul>

When you migrate from a legacy Netezza environment to Azure Synapse, you must consider some specific factors, in addition to the more general subjects described in the Netezza documentation.

## Initial migration workload

Legacy Netezza environments typically evolve over time to encompass multiple subject areas and mixed workloads. When you are deciding where to start on an initial migration project, it makes sense to choose an area that:

- Proves the viability of migrating to Azure Synapse by quickly delivering the benefits of the new environment.
- Allows in-house technical staff to gain experience with new processes and tools so that they can use them to migrate other areas.
- Creates a template based on the current tools and processes to use in additional migration from the source Netezza environment.

A good candidate for an initial migration from a Netezza environment that would support these objectives typically is one that implements a Power BI/analytics workload rather than an OLTP workload. The workload should have a data model that can be migrated with minimal modifications, such as a star or snowflake schema.

For size, it's important that the data volume you migrate in the initial exercise is large enough to demonstrate the capabilities and benefits of the Azure Synapse environment with a short time to demonstrate value. The size that typically meets the requirements is in the range of 1 terabyte (TB) to 10 TB.

An approach for the initial migration project that minimizes risk and implementation time is to confine the scope of the migration to data marts. This approach is a good starting point because it clearly limits the scope of the migration and typically can be achieved on a short timescale. An initial migration of data marts only doesn't address broader concerns like how to migrate ETL and historical data. You must address these areas in later phases and backfill the migrated data mart layer with the data and processes that are required to build them.

## Lift-and-shift approach vs. phased approach

Regardless of the drivers and scope that you choose for your migration, you can choose from two general types of migration:

- **Lift-and-shift approach:** In this approach, the existing data model, such as a star schema, is migrated unchanged to the new Azure Synapse platform. In this scenario, the emphasis is on minimizing risk and the time it takes to migrate by reducing the work that has to be done to achieve the benefits of moving to the Azure cloud environment.

This approach is a good fit for existing Teradata environments in which a single data mart is to be migrated, and if the data is already in a well-designed star or snowflake schema. This approach is a good choice also if you have time and cost pressures to move to a more modern cloud environment.

- **Phased approach that incorporates modifications:** When a legacy warehouse has evolved over time, you might need to reengineer the data warehouse to maintain the required performance or to support new data sources like IoT streams. Migrating to Azure Synapse for the well-known benefits of a scalable cloud environment might be considered part of the reengineering process. This process might include changing the underlying data model, such as moving from an Inmon model to Azure Data Vault.

The approach we recommend is to initially move the existing data model as-is to Azure. Then, take advantage of the performance and flexibility of Azure services to apply the reengineering changes without affecting the existing source system.

## Metadata migration

It makes sense to automate and orchestrate the migration process by using the capabilities of the Azure environment. This approach minimizes the effect on the existing Netezza environment, which might already be running close to full capacity.

Azure Data Factory is a cloud-based data integration service. You can use Data Factory to create data-driven workflows in the cloud to orchestrate and automate data movement and data transformation. Data Factory pipelines can ingest data from disparate datastores, and then process and transform the data by using compute services like Azure HDInsight for Apache Hadoop and Apache Spark, Azure Data Lake Analytics, and Azure Machine Learning. You start by creating metadata to list the data tables you want to migrate, with their locations, and then use Data Factory capabilities to manage the migration process.

## Design differences between Netezza and Azure Synapse

As you plan your migration from a legacy Netezza environment to Azure Synapse, it's important to consider the design differences between the two platforms.

### Multiple databases vs. a single database and schemas

In a Netezza environment, you might have multiple, separate databases for different parts of the overall environment. For example, you might have a separate database for data ingestion and staging tables, a database for core warehouse tables, and another database for data marts, sometimes called a *semantic layer*. Processing separate databases as ETL/ELT pipelines in Azure Synapse might require implementing cross-database joins and moving data between the separate databases.

The Azure Synapse environment has a single database. Schemas are used to separate tables into logically separate groups. We recommend that you use a series of schemas in the target Azure Synapse to mimic any separate databases that you migrate from Netezza. If you use schemas in the Netezza environment, you might need to use a new naming convention to move the existing Netezza tables and views to the new environment. For example, you might concatenate the existing Netezza schema and table names into the new Azure Synapse table name, and then use schema names in the new environment to maintain the original separate database names.

Another option is to use SQL views over the underlying tables to maintain the logical structures. There are some potential downsides to using SQL views:

- Views in Azure Synapse are read-only, so you must make any updates to the data on the underlying base tables.
- If layers of views already exist, adding another layer of views might affect performance.

### Tables

When you migrate tables between different technologies, you physically move only raw data and the metadata that describes it between the two environments. You don't migrate database elements like indexes from the source system because they might not be needed or they might be implemented differently in the new environment.

However, understanding where performance optimizations like indexes have been used in the source environment can be a helpful indication of where you might optimize performance in the new environment. For example, if queries in the source Netezza environment frequently use zone maps, you might conclude that it would be advantageous to create a nonclustered index in the migrated Azure Synapse environment, or that using other native performance optimization techniques like table replication might be preferable to creating a like-for-like index.

### Unsupported Netezza database object types

Netezza implements some database objects that aren't directly supported in Azure Synapse. However, Azure Synapse offers methods that you can use to achieve the same functionality in the new environment, as described in the following list:

- **Zone maps:** In Netezza, zone maps are automatically created and maintained for some column types. Zone maps are used at query time on the following column types to restrict the amount of data to be scanned:
  - `INTEGER` columns that are a length of 8 bytes or less
  - Temporal columns, including `DATE`, `TIME`, and `TIMESTAMP`
  - `CHAR` columns, if they are part of a materialized view and included in the `ORDER BY` clause

You can find out which columns have zone maps by using the `nz_zonemap` utility. The utility is part of the NZ Toolkit.

Azure Synapse doesn't use zone maps, but you can achieve similar results by using user-defined index types or partitioning.

- **Clustered base tables (CBTs):** In Netezza, the most common CBT is the fact table, which has billions of records. Scanning such a huge table requires a long processing time because a full table scan might be needed to get relevant records. By organizing records in restrictive CBTs, Netezza can group records in the same or nearby extents. The process also creates zone maps that improve performance by reducing the amount of data to scan.

In Azure Synapse, you can achieve a similar result through partitioning or by using other index types.

- **Materialized views:** Netezza recommends that users create one or more materialized view over large tables that have many columns, and in which only a few columns are regularly used in queries. Materialized views are automatically maintained by the system when data in the base table is updated.

Currently, Microsoft offers preview support for materialized views, with the same functionality as Netezza, in Azure Synapse.

- **Data type mapping:** Most Netezza data types have a direct equivalent in Azure Synapse. The following table shows the data types and the recommended approaches for mapping the data types.

Some third-party vendors offer tools and services that can automate migration tasks, including data type mapping. If a third-party ETL tool like Informatica or Talend is already used in the Netezza environment, you can use the tool to implement any data transformations that are required.

- **SQL Data Manipulation Language (DML) syntax:** You should be aware of a few differences in SQL DML syntax between Netezza SQL and Azure Synapse.

Here are some key functions and how they are different:

- `STRPOS` : In Netezza, the `STRPOS` function returns the position of a substring within a string. The equivalent in Azure Synapse is the `CHARINDEX` function, and the order of the arguments is reversed.

In Netezza:

```
SELECT STRPOS('abcdef', 'def') ...
```

Is replaced with the following code in Azure Synapse:

```
SELECT CHARINDEX('def', 'abcdef') ...
```

- `AGE` : Netezza supports the `AGE` operator to give the interval between two temporal values (for example, timestamps and dates). For example:

```
SELECT AGE ('23-03-1956', '01-01-2019') FROM ...
```

You can achieve the same result in Azure Synapse by using `DATEDIFF` (note the date representation sequence):

```
SELECT DATEDIFF(day, '1956-03-23', '2019-01-01') FROM ...
```

- `NOW()` : Netezza uses `NOW()` to represent `CURRENT_TIMESTAMP` in Azure Synapse.

## Functions, stored procedures, and sequences

When you migrate a data warehouse from a mature legacy environment like Netezza, you often need to migrate elements other than simple tables and views to the new target environment. Examples of non-table elements in

Netezza that you might need to migrate to Azure Synapse are functions, stored procedures, and sequences. During the preparation phase of the migration, you should create an inventory of objects to migrate. In the project plan, define the method of handling all objects and allocate the appropriate resources for their migration.

You might find services in the Azure environment that replace the functionality implemented as functions or stored procedures in the Netezza environment. Usually, it's more efficient to use the built-in Azure capabilities instead of recoding the Netezza functions.

Also, third-party vendors offer tools and services that can automate the migration of functions, stored procedures, and sequences from Netezza. Examples include Qlik (formerly Attunity) and WhereScape.

Here's some additional information about migrating functions, stored procedures, and sequences:

- **Functions:** Like most database products, Netezza supports system functions and user-defined functions in a SQL implementation. When common system functions are migrated to another database platform like Azure Synapse, they generally are available in the new environment and can be migrated without change. If system functions have slightly different syntax in the new environment, you usually can automate the required changes.

You might need to recode arbitrary user-defined functions and system functions that have no equivalent in the new environment. Use the languages that are available in the new environment. Netezza user-defined functions are coded by using nzLua or C++. Azure Synapse uses the popular Transact-SQL language to implement user-defined functions.

- **Stored procedures:** In most modern database products, you can store procedures in the database. A stored procedure typically contains SQL statements and some procedural logic. It might also return data or a status.

Netezza provides the NZPLSQL language, based on PL/pgSQL, for stored procedures. Azure Synapse supports stored procedures by using T-SQL. If you migrate stored procedures to Azure Synapse, you must recode them by using T-SQL.

- **Sequences:** In Netezza, a sequence is a named database object that's created via a `CREATE SEQUENCE` statement. Objects can provide the unique value via the `NEXT()` method. You can use values to generate unique numbers as surrogate key values for primary key values.

Azure Synapse doesn't support `CREATE SEQUENCE`. In Azure Synapse, sequences are handled by using identity columns or SQL code to create the next sequence number in a series.

## Metadata and data extraction

Consider the following information when you plan how to extract metadata and data from the Netezza environment:

- **Data Definition Language (DDL) generation:** It's possible to edit existing Netezza `CREATE TABLE` and `CREATE VIEW` scripts to create the equivalent definitions, with modified data types if necessary, as described earlier. This task usually involves removing or modifying any clauses that are specific to Netezza, like `ORGANIZE ON`.

In Netezza, the information that specifies the current table and view definitions is maintained in system catalog tables. System catalog tables are the best source of the information because the tables likely are up to date and complete. User-maintained documentation might not be in sync with current table definitions.

You can access system catalog tables in Netezza by using a utility like `nz_ddl_table`. You can use the tables to generate `CREATE TABLE` DDL statements, which you can then edit for the equivalent tables in Azure Synapse. Third-party migration and ETL tools also use the catalog information to achieve the same results.

- **Data extraction:** You can extract raw data to migrate from an existing Netezza table into a flat, delimited file by using standard Netezza utilities like `nzsql` and `nzunload`, and by using external tables. Compress the

files by using gzip, and then use AzCopy or an Azure data transport service like Azure Data Box to upload the files to Azure Blob storage.

During a migration exercise, it's important to extract data as efficiently as possible. The recommended approach for Netezza is to use external tables, which also is the fastest method. You can complete multiple extracts in parallel to maximize the throughput for data extraction.

Here's a simple example of an external table extract:

```
CREATE EXTERNAL TABLE '/tmp/export_tab1.CSV' USING (DELIM ',') AS SELECT * from <TABLE-NAME>;
```

If you have sufficient network bandwidth, you can extract data directly from an on-premises Netezza system into Azure Synapse tables or into Azure data storage by using Data Factory processes or third-party data migration or ETL products.

Recommended data formats for extracted data are delimited text files (also called *comma-separated values*), optimized row columnar files, or Parquet files.

For more detailed information about the process of migrating data and ETL from a Netezza environment, see the Netezza documentation about data migration ETL and load.

## Performance-tuning recommendations

When you move to Azure Synapse from a Netezza environment, many of the performance-tuning concepts you use will be familiar.

For example, these concepts are the same for both environments:

- Data distribution collocates data to be joined onto the same processing node.
- Using the smallest data type for a specific column saves storage space and accelerates query processing.
- Ensuring that data types of columns to be joined are identical optimizes join processing by reducing the need to transform data for matching.
- Ensuring that statistics are up to date helps the optimizer produce the best execution plan.

There are some differences between platforms when it comes to optimization. In the following list of performance-tuning recommendations, lower-level implementation differences between Netezza and Azure Synapse, and alternatives for your migration, are highlighted:

- **Data distribution options:** In both Netezza and Azure Synapse, you can use a `CREATE TABLE` statement to specify a distribution definition. Use `DISTRIBUTE ON` for Netezza and `DISTRIBUTION =` for Azure Synapse.

Azure Synapse provides an additional way to achieve local joins for small table/large table joins, often called a *dimension table/fact table join* in a star schema model. The approach is to replicate the smaller dimension table across all nodes, thereby ensuring that any value of the join key for the larger table will have a matching dimension row that's locally available. The overhead of replicating the dimension table is relatively low if the tables are not large. In this case, using the hash distribution approach described earlier is preferable.

- **Data indexing:** Azure Synapse provides various user-definable indexing options, but the options are different in operation and usage than system-managed zone maps in Netezza. To learn about the indexing options in Azure Synapse, see [Index tables in an Azure Synapse SQL pool](#).

Existing system-managed zone maps in the source Netezza environment can provide a useful indication of how data is used and provide an indication of candidate columns for indexing in the Azure Synapse environment.

- **Data partitioning:** In an enterprise data warehouse, fact tables might contain many billions of rows of data. Partitioning is a way to optimize maintenance and querying in these tables. Splitting the tables into

separate parts reduces the amount of data processed at one time. Partitioning for a table is defined in the `CREATE TABLE` statement.

Only one field per table can be used for partitioning. The field that's used for partitioning frequently is a date field because many queries are filtered by date or by a date range. You can change the partitioning of a table after initial load. To change a table's partitioning, re-create the table with a new distribution that uses the `CREATE TABLE AS SELECT` statement. For a detailed description of partitioning in Azure Synapse, see [Partition tables in an Azure Synapse SQL pool](#).

- **PolyBase for data loading:** PolyBase is the most efficient method to use to load large amounts of data into a warehouse. You can use PolyBase to load data in parallel streams.
- **Resource classes for workload management:** Azure Synapse uses resource classes to manage workloads. In general, large resource classes provide better individual query performance. Smaller resource classes give you higher levels of concurrency. You can use dynamic management views to monitor utilization to help ensure that the appropriate resources are used efficiently.

## Next steps

For more information about implementing a Netezza migration, talk with your Microsoft account representative about on-premises migration offers.

# Azure Synapse Analytics solutions and migration for an Oracle data warehouse

11/9/2020 • 2 minutes to read • [Edit Online](#)

An Oracle data warehouse schema is different from Azure Synapse Analytics in several ways. The differences include databases, data types, and a range of Oracle Database object types that aren't supported in Azure Synapse.

Like other database management systems, when you migrate an Oracle data warehouse to Azure Synapse, you'll find that Oracle has multiple, separate databases and Azure Synapse has only one database. You might need to use a new naming convention, such as concatenating Oracle schema and table names, to move tables and views in your Oracle data warehouse staging database, production database, and data mart databases to Azure Synapse.

Several Oracle Database objects aren't supported in Azure Synapse. Database objects that aren't supported in Azure Synapse include Oracle bit-mapped indexes, function-based indexes, domain indexes, Oracle clustered tables, row-level triggers, user-defined data types, and PL/SQL stored procedures. You can identify these objects by querying various Oracle system catalog tables and views. In some cases, you can use workarounds. For example, you can use partitioning or other index types in Azure Synapse to work around the unsupported index types in Oracle. You might be able to use materialized views instead of Oracle clustered tables, and migration tools like SQL Server Migration Assistant (SSMA) for Oracle can translate at least some PL/SQL.

When you migrate an Oracle data warehouse schema, you also must take into account data type differences on columns. To find the columns in your Oracle data warehouse and data mart schemas that have data types that don't map to data types in Azure Synapse, query the Oracle catalog. You can use workarounds for several of these instances.

To maintain or improve performance of your schema after migration, consider performance mechanisms, like Oracle indexing, that you currently have in place. For example, bit-mapped indexes that Oracle queries frequently use might indicate that creating a nonclustered index in the migrated schema on Azure Synapse would be advantageous.

A good practice in Azure Synapse includes using data distribution to colocate data to be joined onto the same processing node. Another good practice in Azure Synapse is ensuring that data types of columns to be joined are identical. Using identical joined columns optimizes join processing by reducing the need to transform data for matching. In Azure Synapse, often it isn't necessary to migrate every Oracle index because other features provide high performance. You can instead use parallel query processing, in-memory data, and result set caching and data distribution options that reduce I/O.

SSMA for Oracle can help you migrate an Oracle data warehouse or data mart to Azure Synapse. SSMA is designed to automate the process of migrating tables, views, and data from an existing Oracle environment. Among other features, SSMA recommends index types and data distributions for target Azure Synapse tables, and it applies data type mappings during migration. Although SSMA isn't the most efficient approach for very high volumes of data, it's useful for smaller tables.

# Mainframe migration overview

11/9/2020 • 4 minutes to read • [Edit Online](#)

Many companies and organizations benefit from moving some or all their mainframe workloads, applications, and databases to the cloud. Azure provides mainframe-like features at cloud scale without many of the drawbacks associated with mainframes.

The term mainframe generally refers to a large computer system, but the vast majority currently of mainframes deployed are IBM System Z servers or IBM plug-compatible systems running MVS, DOS, VSE, OS/390, or z/OS. Mainframe systems continue to be used in many industries to run vital information systems, and they have a place in highly specific scenarios, such as large, high-volume, transaction-intensive IT environments.

Migrating to the cloud enables companies to modernize their infrastructure. With cloud services you can make mainframe applications, and the value that they provide, available as a workload whenever your organization needs it. Many workloads can be transferred to Azure with only minor code changes, such as updating the names of databases. You can migrate more complex workloads using a phased approach.

Most Fortune 500 companies are already running Azure for their critical workloads. Azure's significant bottom-line incentives motivate many migration projects. Companies typically move development and test workloads to Azure first, followed by DevOps, email, and disaster recovery.

## Intended audience

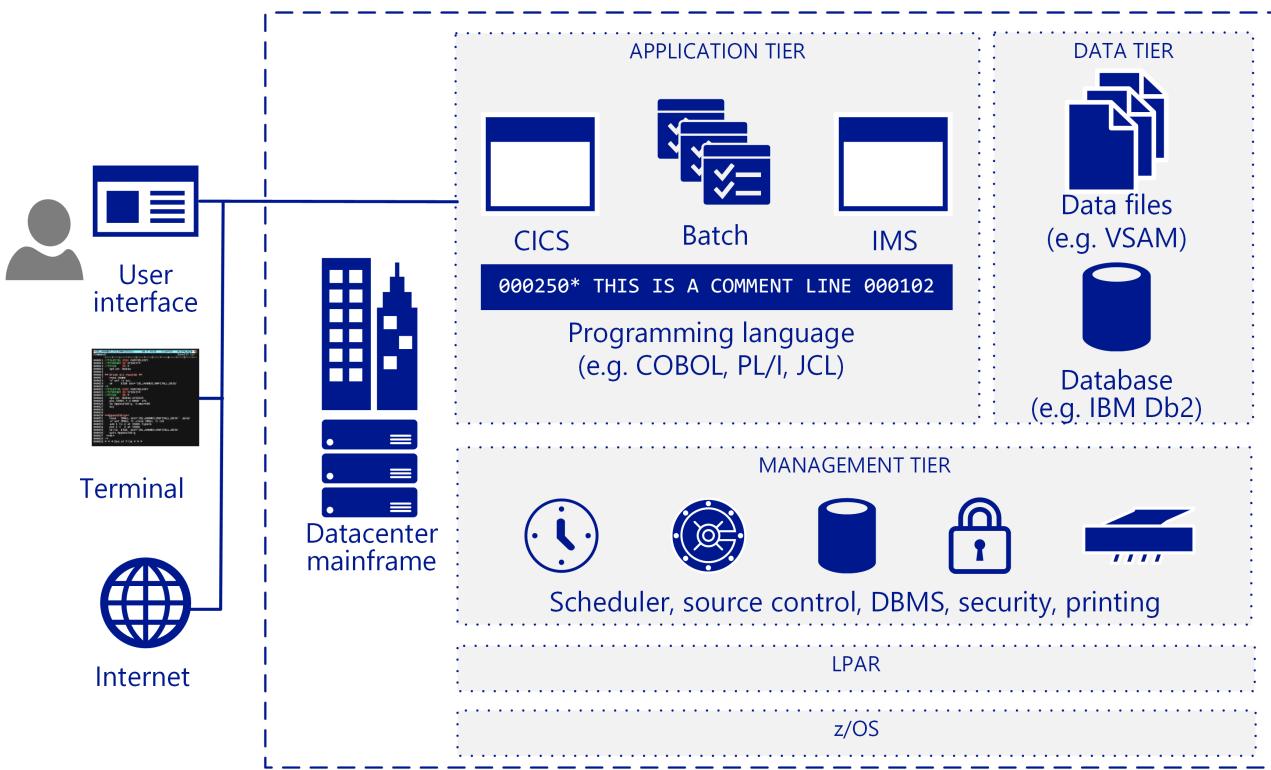
If you're considering a migration or the addition of cloud services as an option for your IT environment, this guide is for you.

This guidance helps IT organizations start the migration conversation. You may be more familiar with Azure and cloud-based infrastructures than you are with mainframes, so this guide starts with an overview of how mainframes work, and continues with various strategies for determining what and how to migrate.

## Mainframe architecture

In the late 1950s, mainframes were designed as scale-up servers to run high-volume online transactions and batch processing. Because of this, mainframes have software for online transaction forms (sometimes called green screens) and high-performance I/O systems for processing batch runs.

Mainframes are known for high reliability and availability as well as their ability to run huge online transactions and batch jobs. A transaction results from a piece of processing initiated by a single request, typically from a user at a terminal. Transactions can also come from multiple other sources, including web pages, remote workstations, and applications from other information systems. A transaction can also be triggered automatically at a predefined time as the following figure shows.



A typical IBM mainframe architecture includes these common components:

- **Front-end systems:** Users can initiate transactions from terminals, web pages, or remote workstations. Mainframe applications often have custom user interfaces that can be preserved after migration to Azure. Terminal emulators (also called green-screen terminals) are still used to access mainframe applications.
- **Application tier:** Mainframes typically include a customer information control system (CICS), a leading transaction management suite for the IBM z/OS mainframe that is often used with IBM Information Management System (IMS), a message-based transaction manager. Batch systems handle high-throughput data updates for large volumes of account records.
- **Code:** Programming languages used by mainframes include COBOL, Fortran, PL/I, and Natural. Job control language (JCL) is used to work with z/OS.
- **Database tier:** A common relational database management system (DBMS) for z/OS is IBM DD2. It manages data structures called *dbspaces* that contain one or more tables and are assigned to storage pools of physical data sets called *dbextents*. Two important database components are the directory that identifies data locations in the storage pools, and the log that contains a record of operations performed on the database. Various flat-file data formats are supported. DB2 for z/OS typically uses virtual storage access method (VSAM) datasets to store the data.
- **Management tier:** IBM mainframes include scheduling software such as TWS-OPC, tools for print and output management such as CA-SAR and SPOOL, and a source control system for code. Secure access control for z/OS is handled by resource access control facility (RACF). A database manager provides access to data in the database and runs in its own partition in a z/OS environment.
- **LPAR:** Logical partitions, or LPARs, are used to divide compute resources. A physical mainframe is partitioned into multiple LPARs.
- **z/OS:** A 64-bit operating system that is most commonly used for IBM mainframes.

IBM systems use a transaction monitor such as CICS to track and manage all aspects of a business transaction. CICS manages the sharing of resources, the integrity of data, and prioritization of execution. CICS authorizes users, allocates resources, and passes database requests by the application to a database manager, such as IBM DB2.

For more precise tuning, CICS is commonly used with IMS/TM (formerly IMS/Data Communications or IMS/DC).

IMS was designed to reduce data redundancy by maintaining a single copy of the data. It complements CICS as a transaction monitor by maintaining state throughout the process and recording business functions in a data store.

## Mainframe operations

The following are typical mainframe operations:

- **Online:** Workloads include transaction processing, database management, and connections. They are often implemented using IBM DB2, CICS, and z/OS connectors.
- **Batch:** Jobs run without user interaction, typically on a regular schedule such as every weekday morning. Batch jobs can be run on systems based on Windows or Linux by using a JCL emulator such as Micro Focus Enterprise Server or BMC Control-M software.
- **Job control language (JCL):** Specify resources needed to process batch jobs. JCL conveys this information to z/OS through a set of job control statements. Basic JCL contains six types of statements: JOB, ASSGN, DLBL, EXTENT, LIBDEF, and EXEC. A job can contain several EXEC statements (steps), and each step could have several LIBDEF, ASSGN, DLBL, and EXTENT statements.
- **Initial program load (IPL):** Refers to loading a copy of the operating system from disk into a processor's real storage and running it. IPLs are used to recover from downtime. An IPL is like booting the operating system on Windows or Linux VMs.

## Next steps

[Myths and facts](#)

# Mainframe myths and facts

11/9/2020 • 2 minutes to read • [Edit Online](#)

Mainframes figure prominently in the history of computing and remain viable for highly specific workloads. Most agree that mainframes are a proven platform with long-established operating procedures that make them reliable, robust environments. Software runs based on usage, measured in million instructions per second (MIPS), and extensive usage reports are available for chargebacks.

The reliability, availability, and processing power of mainframes have taken on almost mythical proportions. To evaluate the mainframe workloads that are most suitable for Azure, you first want to distinguish the myths from the reality.

## Myth: Mainframes never go down and have a minimum of five 9s of availability

Mainframe hardware and operating systems are viewed as reliable and stable. But the reality is that downtime must be scheduled for maintenance and reboots, referred to as initial program loads (IPLs). When these tasks are considered, a mainframe solution often has closer to two or three 9s of availability, which is equivalent to that of high-end, Intel-based servers.

Mainframes also remain as vulnerable to disasters as any other servers do, and require uninterruptible power supply (UPS) systems to handle these types of failures.

## Myth: Mainframes have limitless scalability

A mainframe's scalability depends on the capacity of its system software, such as the customer information control system (CICS), and the capacity of new instances of mainframe engines and storage. Some large companies that use mainframes have customized their CICS for performance, and have otherwise outgrown the capability of the largest available mainframes.

## Myth: Intel-based servers are not as powerful as mainframes

The new core-dense, Intel-based systems have as much compute capacity as mainframes.

## Myth: The cloud can't accommodate mission-critical applications for large companies such as financial institutions

Although there may be some isolated instances where cloud solutions fall short, it is usually because the application algorithms cannot be distributed. These few examples are the exceptions, not the rule.

## Summary

By comparison, Azure offers an alternative platform that is capable of delivering equivalent mainframe functionality and features, and at a much lower cost. In addition, the total cost of ownership (TCO) of the cloud's subscription-based, usage-driven cost model is far less expensive than mainframe computers.

## Next steps

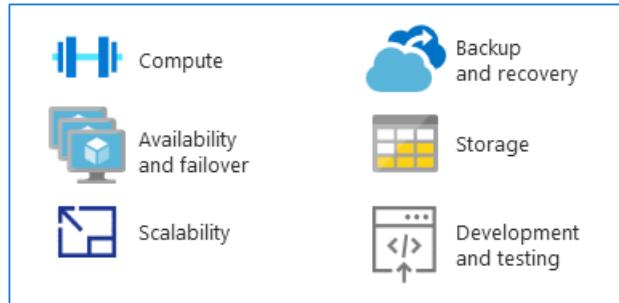
[Make the switch from mainframes to Azure](#)

# Make the switch from mainframes to Azure

11/9/2020 • 4 minutes to read • [Edit Online](#)

As an alternative platform for running traditional mainframe applications, Azure offers hyperscale compute and storage in a high availability environment. You get the value and agility of a modern, cloud-based platform without the costs associated with a mainframe environment.

This section provides technical guidance for making the switch from a mainframe platform to Azure.



## MIPS vs. vCPUs

There is no universal mapping formula that exists for determining the number of virtual central processing units (vCPUs) needed to run mainframe workloads. However, the metric of a million instructions per second (MIPS) is often mapped to vCPUs on Azure. MIPS measures the overall compute power of a mainframe by providing a constant value of the number of cycles per second for a given machine.

A small organization might require less than 500 MIPS, while a large organization typically uses more than 5,000 MIPS. At \$1,000 per single MIPS, a large organization spends approximately \$5 million annually to deploy a 5,000-MIPS infrastructure. The annual cost estimate for a typical Azure deployment of this scale is approximately one-tenth the cost of a MIPS infrastructure. For details, see Table 4 in the [Demystifying Mainframe-to-Azure Migration](#) white paper.

An accurate calculation of MIPS to vCPUs with Azure depends on the type of vCPU and the exact workload you are running. However, benchmark studies provide a good basis for estimating the number and type of vCPUs you will need. A recent HPE zREF benchmark provides the following estimates:

- 288 MIPS per Intel-based core running on HP Proliant servers for online (CICS) jobs.
- 170 MIPS per Intel core for COBOL batch jobs.

This guide estimates 200 MIPS per vCPU for online processing and 100 MIPS per vCPU for batch processing.

### NOTE

These estimates are subject to change as new virtual machine (VM) series become available in Azure.

## High availability and failover

Mainframe systems often offer five 9s availability (99.999 percent) when mainframe coupling and Parallel Sysplex are used. Yet system operators still need to schedule downtime for maintenance and initial program loads (IPLs). The actual availability approaches two or three 9s, comparable to high end, Intel-based servers.

By comparison, Azure offers commitment-based service level agreements (SLAs), where multiple 9s availability is

the default, optimized with local or geo-based replication of services.

Azure provides additional availability by replicating data from multiple storage devices, either locally or in other geographic regions. In the event of an Azure-based failure, compute resources can access the replicated data on either the local or regional level.

When you use Azure platform as a service (PaaS) resources, such as [Azure SQL Database](#) and [Azure Cosmos Database](#), Azure can automatically handle failovers. When you use Azure infrastructure as a service (IaaS), failover relies on specific system functionality, such as SQL Server Always On features, failover clustering instances, and availability groups.

## Scalability

Mainframes typically scale up, while cloud environments scale out. Mainframes can scale out with the use of a coupling facility (CF), but the high cost of hardware and storage makes mainframes expensive to scale out.

A CF also offers tightly coupled compute, whereas the scale-out features of Azure are loosely coupled. The cloud can scale up or down to match exact user specifications, with compute power, storage, and services scaling on demand under a usage-based billing model.

## Backup and recovery

Mainframe customers typically maintain disaster recovery sites or make use of an independent mainframe provider for disaster contingencies. Synchronization with a disaster recovery site is usually done through offline copies of data. Both options incur high costs.

Automated geo-redundancy is also available through the mainframe coupling facility. This approach is expensive and is typically reserved for mission-critical systems. In contrast, Azure has easy-to-implement and cost-effective options for [backup](#), [recovery](#), and [redundancy](#) at local or regional levels, or via geo-redundancy.

## Storage

Part of understanding how mainframes work involves decoding various overlapping terms. For example, central storage, real memory, real storage, and main storage all generally refer to storage attached directly to the mainframe processor.

Mainframe hardware includes processors and many other devices, such as direct-access storage devices (DASDs), magnetic tape drives, and several types of user consoles. Tapes and DASDs are used for system functions and by user programs.

Types of physical storage for mainframes include:

- **Central storage:** Located directly on the mainframe processor, this is also known as processor or real storage.
- **Auxiliary storage:** Located separately from the mainframe, this type includes storage on DASDs and is also known as paging storage.

The cloud offers a range of flexible, scalable options, and you will pay only for those options that you need. [Azure Storage](#) offers a massively scalable object store for data objects, a file system service for the cloud, a reliable messaging store, and a NoSQL store. For VMs, managed and unmanaged disks provide persistent, secure disk storage.

## Mainframe development and testing

A major driver in mainframe migration projects is the changing face of application development. Organizations want their development environment to be more agile and responsive to business needs.

Mainframes typically have separate logical partitions (LPARs) for development and testing, such as QA and staging

LPARs. Mainframe development solutions include compilers (COBOL, PL/I, Assembler) and editors. The most common is the Interactive System Productivity Facility (ISPF) for the z/OS operating system that runs on IBM mainframes. Others include ROSCOE Programming Facility (RPF) and Computer Associates tools, such as CA Librarian and CA-Panvalet.

Emulation environments and compilers are available on x86 platforms, so development and testing can typically be among the first workloads to migrate from a mainframe to Azure. The availability and widespread use of [DevOps tools in Azure](#) is accelerating the migration of development and testing environments.

When solutions are developed and tested on Azure and are ready for deployment to the mainframe, you will need to copy the code to the mainframe and compile it there.

## Next steps

[Mainframe application migration](#)

# Mainframe application migration

11/9/2020 • 10 minutes to read • [Edit Online](#)

When migrating applications from mainframe environments to Azure, most teams follow a pragmatic approach: reuse wherever and whenever possible, and then start a phased deployment where applications are rewritten or replaced.

Application migration typically involves one or more of the following strategies:

- **Rehost:** You can move existing code, programs, and applications from the mainframe, and then recompile the code to run in a mainframe emulator hosted in a cloud instance. This approach typically starts with moving applications to a cloud-based emulator, and then migrating the database to a cloud-based database. Some engineering and refactoring are required along with data and file conversions.  
Alternatively, you can rehost using a traditional hosting provider. One of the principal benefits of the cloud is outsourcing infrastructure management. You can find a datacenter provider that will host your mainframe workloads for you. This model may buy time, reduce vendor lock in, and produce interim cost savings.
- **Retire:** All applications that are no longer needed should be retired before migration.
- **Rebuild:** Some organizations choose to completely rewrite programs using modern techniques. Given the added cost and complexity of this approach, it's not as common as a lift and shift approach. Often after this type of migration, it makes sense to begin replacing modules and code using code transformation engines.
- **Replace:** This approach replaces mainframe functionality with equivalent features in the cloud. Software as a service (SaaS) is one option, which is using a solution created specifically for an enterprise concern, such as finance, human resources, manufacturing, or enterprise resource planning. In addition, many industry-specific apps are now available to solve problems that custom mainframe solutions used to previously solve.

You should consider starting by planning those workloads that you want to initially migrate, and then determine those requirements for moving associated applications, legacy code bases, and databases.

## Mainframe emulation in Azure

Azure cloud services can emulate traditional mainframe environments, enabling you to reuse existing mainframe code and applications. Common server components that you can emulate include online transaction processing (OLTP), batch, and data ingestion systems.

### OLTP systems

Many mainframes have OLTP systems that process thousands or millions of updates for huge numbers of users. These applications often use transaction processing and screen-form handling software, such as customer information control system (CICS), information management systems (IMS), and terminal interface processor (TIP).

When moving OLTP applications to Azure, emulators for mainframe transaction processing (TP) monitors are available to run as infrastructure as a service (IaaS) using virtual machines (VMs) on Azure. The screen handling and form functionality can also be implemented by web servers. This approach can be combined with database APIs, such as ActiveX data objects (ADO), open database connectivity (ODBC), and Java database connectivity (JDBC) for data access and transactions.

### Time-constrained batch updates

Many mainframe systems perform monthly or annual updates of millions of account records, such as those used in banking, insurance, and government. Mainframes handle these types of workloads by offering high-throughput data handling systems. Mainframes batch jobs are typically serial in nature and depend on the input/output

operations per second (IOPS) provided by the mainframe backbone for performance.

Cloud-based batch environments use parallel compute and high-speed networks for performance. If you need to optimize batch performance, Azure provides various compute, storage, and networking options.

### Data ingestion systems

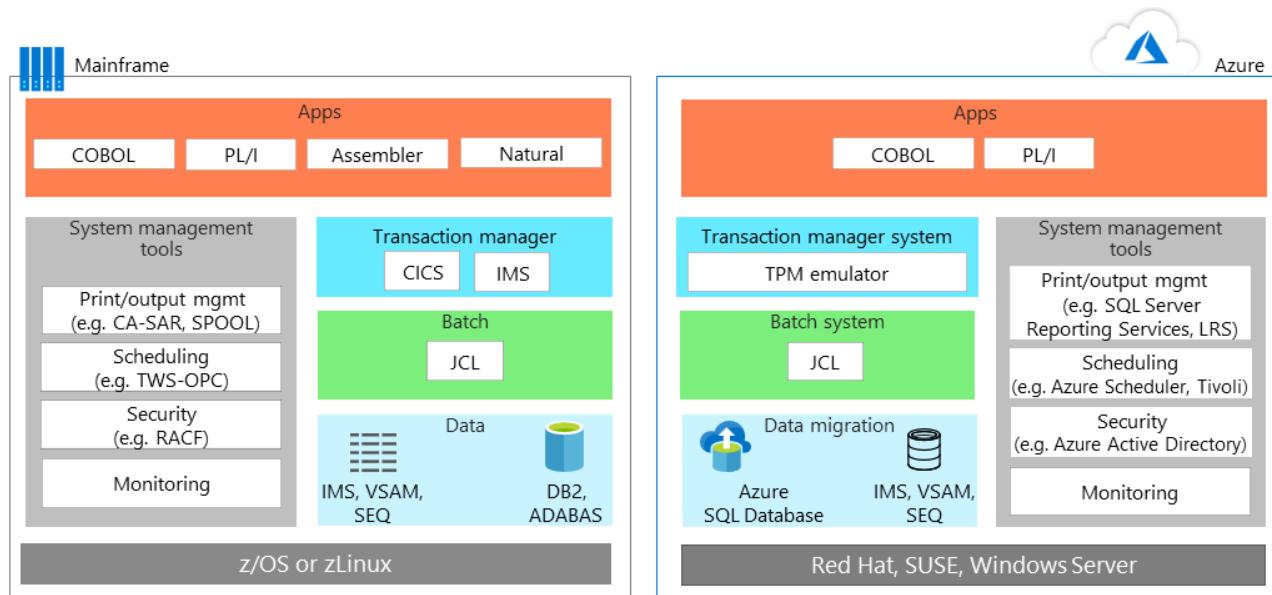
Mainframes ingest large batches of data from retail, financial services, manufacturing, and other solutions for processing. With Azure, you can use simple command-line utilities such as [AzCopy](#) for copying data to and from storage location. You can also use the [Azure Data Factory](#) service, enabling you to ingest data from disparate data stores to create and schedule data-driven workflows.

In addition to emulation environments, Azure provides platform as a service (PaaS) and analytics services that can enhance existing mainframe environments.

## Migrate OLTP workloads to Azure

The lift and shift approach is the no-code option for quickly migrating existing applications to Azure. Each application is migrated as is, which provides the benefits of the cloud without the risks or costs of making code changes. Using an emulator for mainframe transaction processing (TP) monitors on Azure supports this approach.

TP monitors are available from various vendors and run on virtual machines, an infrastructure as a service (IaaS) option on Azure. The following before and after diagrams show a migration of an online application backed by IBM DB2, a relational database management system (DBMS), on an IBM z/OS mainframe. DB2 for z/OS uses virtual storage access method (VSAM) files to store the data and Indexed Sequential Access Method (ISAM) for flat files. This architecture also uses CICS for transaction monitoring.



On Azure, emulation environments are used to run the TP manager and the batch jobs that use JCL. In the data tier, DB2 is replaced by [Azure SQL Database](#), although Microsoft SQL Server, DB2 LUW, or Oracle Database can also be used. An emulator supports IMS, VSAM, and SEQ. The mainframe's system management tools are replaced by Azure services, and software from other vendors, that run in VMs.

The screen handling and form entry functionality is commonly implemented using web servers, which can be combined with database APIs, such as ADO, ODBC, and JDBC for data access and transactions. The exact line-up of Azure IaaS components to use depends on the operating system you prefer. For example:

- Windows-based VMs: Internet Information Server (IIS) along with ASP.NET for the screen handling and business logic. Use ADO.NET for data access and transactions.
- Linux-based VMs: The Java-based application servers that are available, such as Apache Tomcat for screen handling and Java-based business functionality. Use JDBC for data access and transactions.

# Migrate batch workloads to Azure

Batch operations in Azure differ from the typical batch environment on mainframes. Mainframe batch jobs are typically serial in nature and depend on the IOPS provided by the mainframe backbone for performance. Cloud-based batch environments use parallel computing and high-speed networks for performance.

To optimize batch performance using Azure, consider the [compute](#), [storage](#), [networking](#), and [monitoring](#) options as follows.

## Compute

Use:

- VMs with the highest clock speed. Mainframe applications are often single-threaded and mainframe CPUs have a very high clock speed.
- VMs with large memory capacity to allow caching of data and application work areas.
- VMs with higher density vCPUs to take advantage of multithreaded processing if the application supports multiple threads.
- Parallel processing, as Azure easily scales out for parallel processing, delivering more compute power for a batch run.

## Storage

Use:

- [Azure premium SSD](#) or [Azure ultra SSD](#) for maximum available IOPS.
- Striping with multiple disks for more IOPS per storage size.
- Partitioning for storage to spread IO over multiple Azure storage devices.

## Networking

- Use [Azure Accelerated Networking](#) to minimize latency.

## Monitoring

- Use monitoring tools, [Azure Monitor](#), [Application Insights](#), and Azure logs enable administrators to monitor any over performance of batch runs and help eliminate bottlenecks.

# Migrate development environments

The cloud's distributed architectures rely on a different set of development tools that provide the advantage of modern practices and programming languages. To ease this transition, you can use a development environment with other tools that are designed to emulate IBM z/OS environments. The following list shows options from Microsoft and other vendors:

COMPONENT	AZURE OPTIONS
z/OS	Windows, Linux, or UNIX
CICS	Azure services offered by Micro Focus, Oracle, GT Software (Fujitsu), TmaxSoft, Raincode, and NTT Data, or rewrite using Kubernetes
IMS	Azure services offered by Micro Focus and Oracle

COMPONENT	AZURE OPTIONS
Assembler	Azure services from Raincode and TmaxSoft; or COBOL, C, or Java, or map to operating system functions
JCL	JCL, PowerShell, or other scripting tools
COBOL	COBOL, C, or Java
Natural	Natural, COBOL, C, or Java
FORTRAN and PL/I	FORTRAN, PL/I, COBOL, C, or Java
REXX and PL/I	REXX, PowerShell, or other scripting tools

## Migrate databases and data

Application migration usually involves rehosting the data tier. You can migrate SQL Server, open-source, and other relational databases to fully managed solutions on Azure, such as [Azure SQL Managed Instance](#), [Azure Database for PostgreSQL](#), and [Azure Database for MySQL](#) with [Azure Database Migration Service](#).

For example, you can migrate if the mainframe data tier uses:

- IBM DB2 or an IMS database, use Azure SQL database, SQL Server, DB2 LUW, or Oracle Database on Azure.
- VSAM and other flat files, use Indexed Sequential Access Method (ISAM) flat files for Azure SQL, SQL Server, DB2 LUW, or Oracle.
- Generation Date Groups (GDGs), migrate to files on Azure that use a naming convention and filename extensions that provide similar functionality to GDGs.

The IBM data tier includes several key components that you must also migrate. For example, when you migrate a database, you also migrate a collection of data contained in pools, each containing dbextents, which are z/OS VSAM data sets. Your migration must include the directory that identifies data locations in the storage pools. Also, your migration plan must consider the database log, which contains a record of operations performed on the database. A database can have one, two (dual or alternate), or four (dual and alternate) logs.

Database migration also includes these components:

- **Database manager:** Provides access to data in the database. The database manager runs in its own partition in a z/OS environment.
- **Application requester:** Accepts requests from applications before passing them to an application server.
- **Online resource adapter:** Includes application requester components for use in CICS transactions.
- **Batch resource adapter:** Implements application requester components for z/OS batch applications.
- **Interactive SQL (ISQL):** Runs as a CICS application and interface enabling users to enter SQL statements or operator commands.
- **CICS application:** Runs under the control of CICS, using available resources and data sources in CICS.
- **Batch application:** Runs process logic without interactive communication with users to, for example, produce bulk data updates or generate reports from a database.

## Optimize scale and throughput for Azure

Generally speaking, mainframes scale up, while the cloud scales out. To optimize scale and throughput of mainframe-style applications running on Azure, it is important that you understand at how mainframes can

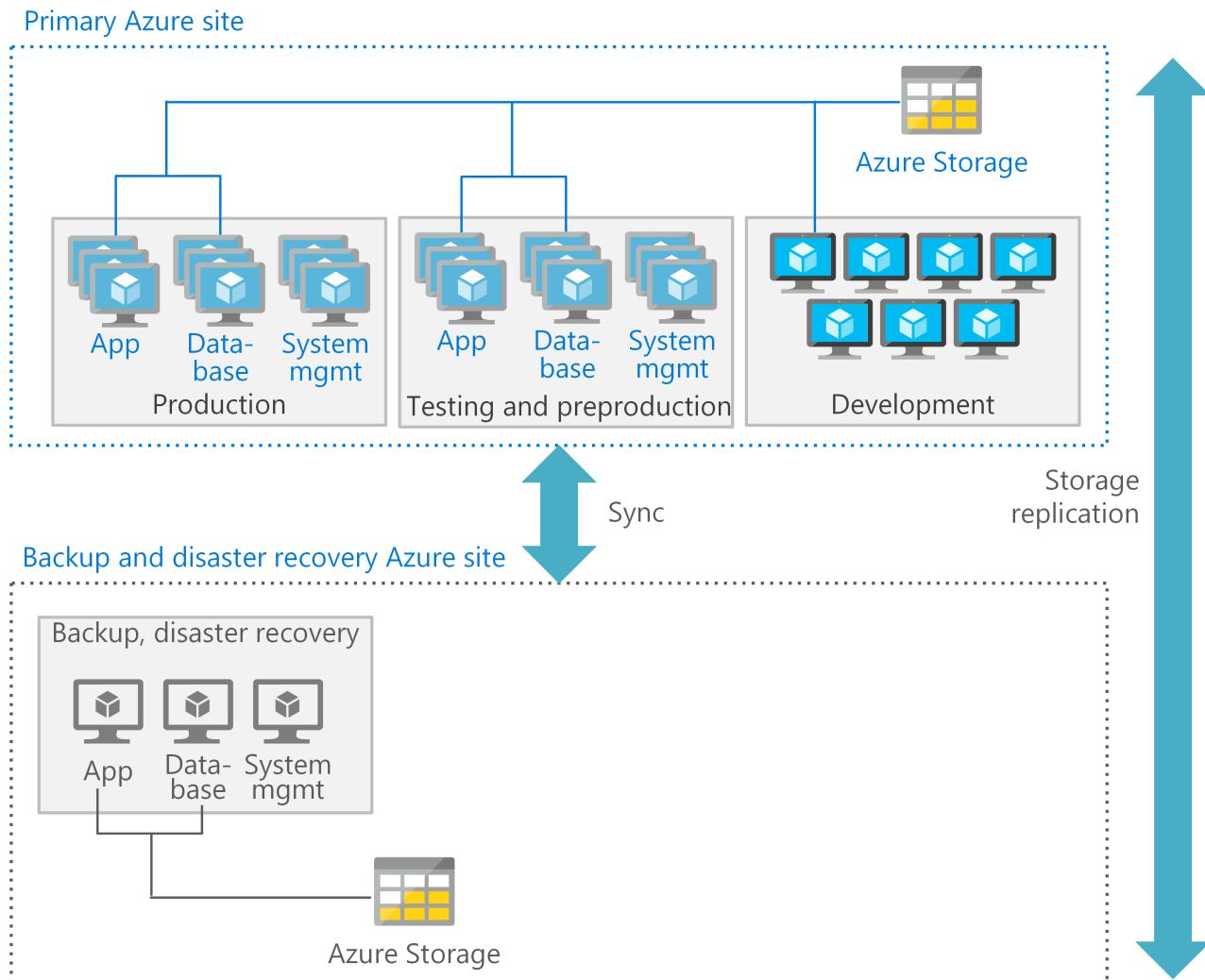
separate and isolate applications. A z/OS mainframe uses a feature called Logical Partitions (LPARS) to isolate and manage the resources for a specific application on a single instance.

For example, a mainframe might use one logical partition (LPAR) for a CICS region with associated COBOL programs, and a separate LPAR for DB2. Additional LPARs are often used for the development, testing, and staging environments.

On Azure, it's more common to use separate VMs to serve this purpose. Azure architectures typically deploy VMs for the application tier, a separate set of VMs for the data tier, another set for development, and so on. Each tier of processing can be optimized using the most suitable type of VMs and features for that environment.

In addition, each tier can also provide appropriate disaster recovery services. For example, production and database VMs might require a hot or warm recovery, while the development and testing VMs support a cold recovery.

The following figure shows a possible Azure deployment using a primary and a secondary site. In the primary site, the production, staging, and testing VMs are deployed with high availability. The secondary site is for backup and disaster recovery.



## Perform a staged mainframe to Azure

Moving solutions from a mainframe to Azure may involve a *staged* migration, whereby some applications are moved first, and others remain on the mainframe temporarily or permanently. This approach typically requires systems that allow applications and databases to interoperate between the mainframe and Azure.

A common scenario is to move an application to Azure while keeping the data used by the application on the mainframe. Specific software is used to enable the applications on Azure to access data from the mainframe.

Fortunately, a wide range of solutions provide integration between Azure and existing mainframe environments, support for hybrid scenarios, and migration over time. Microsoft partners, independent software vendors, and system integrators can help you on your journey.

One option is [Microsoft Host Integration Server](#), a solution that provides the distributed relational database architecture (DRDA) required for applications in Azure to access data in DB2 that remains on the mainframe. Other options for mainframe-to-Azure integration include solutions from IBM, Attunity, Codit, other vendors, and open source options.

## Partner solutions

If you are considering a mainframe migration, the partner ecosystem is available to assist you.

Azure provides a proven, highly available, and scalable infrastructure for systems that currently run on mainframes. Some workloads can be migrated with relative ease. Other workloads that depend on legacy system software, such as CICS and IMS, can be rehosted using partner solutions and migrated to Azure over time. Regardless of the choice you make, Microsoft and our partners are available to assist you in optimizing for Azure while maintaining mainframe system software functionality.

## Learn more

For more information, see the following resources:

- [Get started with Azure](#)
- [Deploy IBM DB2 pureScale on Azure](#)
- [Host Integration Server documentation](#)

# Best practices to secure and manage workloads migrated to Azure

11/9/2020 • 29 minutes to read • [Edit Online](#)

As you plan and design for migration, in addition to thinking about the migration itself, you need to consider your security and management model in Azure after migration. This article describes planning and best practices for securing your Azure deployment after migrating. It also covers ongoing tasks to keep your deployment running at an optimal level.

## IMPORTANT

The best practices and opinions described in this article are based on the Azure platform and service features available at the time of writing. Features and capabilities change over time.

## Secure migrated workloads

After migration, the most critical task is to secure migrated workloads from internal and external threats. These best practices help you to do that:

- Learn how to work with the monitoring, assessments, and recommendations provided by Azure Security Center.
- Get best practices for encrypting your data in Azure.
- Protect your VMs from malware and malicious attacks.
- Keep sensitive information secure in migrated web apps.
- Verify who can access your Azure subscriptions and resources after migration.
- Review your Azure auditing and security logs on a regular basis.
- Understand and evaluate advanced security features that Azure offers.

These best practices are described in more detail in the sections that follow.

## Best practice: Follow Azure Security Center recommendations

Azure tenant admins need to enable security features that protect workloads from attacks. Azure Security Center provides unified security management. From Security Center, you can apply security policies across workloads, limit threat exposure, and detect and respond to attacks. Security Center analyzes resources and configurations across Azure tenants, and makes security recommendations, including:

- **Centralized policy management:** Ensure compliance with company or regulatory security requirements by centrally managing security policies across all your hybrid cloud workloads.
- **Continuous security assessment:** Monitor the security posture of machines, networks, storage and data services, and applications to discover potential security issues.
- **Actionable recommendations:** Remediate security vulnerabilities before they can be exploited by attackers, with prioritized and actionable security recommendations.
- **Prioritized alerts and incidents:** Focus on the most critical threats first, with prioritized security alerts and incidents.

In addition to assessments and recommendations, Azure Security Center provides other security features that you can enable for specific resources.

- **Just-in-time (JIT) access.** Reduce your network attack surface with just-in-time, controlled access to management ports on Azure VMs.
  - Having VM RDP port 3389 open on the internet exposes VMs to continual activity from bad actors. Azure IP addresses are well-known, and hackers continually probe them for attacks on open 3389 ports.
  - Just-in-time uses network security groups (NSGs) and incoming rules that limit the amount of time that a specific port is open.
  - With just-in-time access enabled, Security Center checks that a user has role-based access control (RBAC) write access permissions for a VM. In addition, you can specify rules for how users can connect to VMs. If permissions are OK, an access request is approved, and Security Center configures NSGs to allow inbound traffic to the selected ports for the amount of time you specify. NSGs return to their previous state when the time expires.
- **Adaptive application controls.** Keep software and malware off VMs by controlling which applications run on them, by using dynamic allow lists.
  - Adaptive application controls allow you to approve applications, and prevent rogue users or administrators from installing unapproved or vetted software applications on your VMs.
  - You can block or alert attempts to run malicious applications, avoid unwanted or malicious applications, and ensure compliance with your organization's application security policy.
- **File Integrity Monitoring.** Ensure the integrity of files running on VMs.
  - You don't need to install software to cause VM issues. Changing a system file can also cause VM failure or performance degradation. File Integrity Monitoring examines system files and registry settings for changes, and notifies you if something is updated.
  - Security Center recommends which files you should monitor.

**Learn more:**

- Learn more about [Azure Security Center](#).
- Learn more about [just-in-time VM access](#).
- Learn about [applying adaptive application controls](#).
- [Get started](#) with File Integrity Monitoring.

## Best practice: Encrypt data

Encryption is an important part of Azure security practices. Ensuring that encryption is enabled at all levels helps prevent unauthorized parties from gaining access to sensitive data, including data in transit and at rest.

### Encryption for infrastructure as a service (IaaS)

- **Virtual machines:** For VMs, you can use Azure Disk Encryption to encrypt your Windows and Linux IaaS VM disks.
  - Azure Disk Encryption uses BitLocker for Windows, and dm-crypt for Linux, to provide volume encryption for the operating system and data disks.
  - You can use an encryption key created by Azure, or you can supply your own encryption keys, safeguarded in Azure Key Vault.
  - With Azure Disk Encryption, IaaS VM data is secured at rest (on the disk) and during VM boot.
    - Azure Security Center alerts you if you have VMs that aren't encrypted.
- **Storage:** Protect at-rest data stored in Azure Storage.
  - Data stored in Azure Storage accounts can be encrypted by using Microsoft-generated AES keys that are FIPS 140-2 compliant, or you can use your own keys.
  - Azure Storage encryption is enabled for all new and existing storage accounts, and it can't be disabled.

### Encryption for platform as a service (PaaS)

Unlike IaaS, in which you manage your own VMs and infrastructure, in a PaaS model platform and infrastructure is

managed by the provider. You can focus on core application logic and capabilities. With so many different types of PaaS services, each service is evaluated individually for security purposes. As an example, let's see how you might enable encryption for Azure SQL Database.

- **Always Encrypted:** Use the Always Encrypted Wizard in SQL Server Management Studio to protect data at rest.
  - You create an Always Encrypted key to encrypt individual column data.
  - Always Encrypted keys can be stored as encrypted in database metadata, or stored in trusted key stores such as Azure Key Vault.
  - Most likely, to use this feature, you'll need to make application changes.
- **Transparent data encryption (TDE):** Protect the Azure SQL Database with real-time encryption and decryption of the database, associated backups, and transaction log files at rest.
  - TDE allows encryption activities to take place without changes at the application layer.
  - TDE can use encryption keys provided by Microsoft, or you can bring your own key.

#### Learn more:

- Learn about [Azure Disk Encryption for virtual machines and virtual machine scale sets](#).
- Enable [Azure Disk Encryption for Windows VMs](#).
- Learn about [Azure Storage encryption for data at rest](#).
- Read the [Always Encrypted overview](#).
- Read about [transparent data encryption for SQL Database and Azure synapse](#).
- Learn about [Azure SQL transparent data encryption with customer-managed key](#).

## Best practice: Protect VMs with antimalware

In particular, older Azure-migrated VMs might not have the appropriate level of antimalware installed. Azure provides a free endpoint solution that helps protect VMs from viruses, spyware, and other malware.

- Microsoft Antimalware for Azure Cloud Services and Virtual Machines generates alerts when known malicious or unwanted software tries to install itself.
- It's a single agent solution that runs in the background, without human intervention.
- In Azure Security Center, you can easily identify VMs that don't have endpoint protection running, and install Microsoft antimalware as needed.

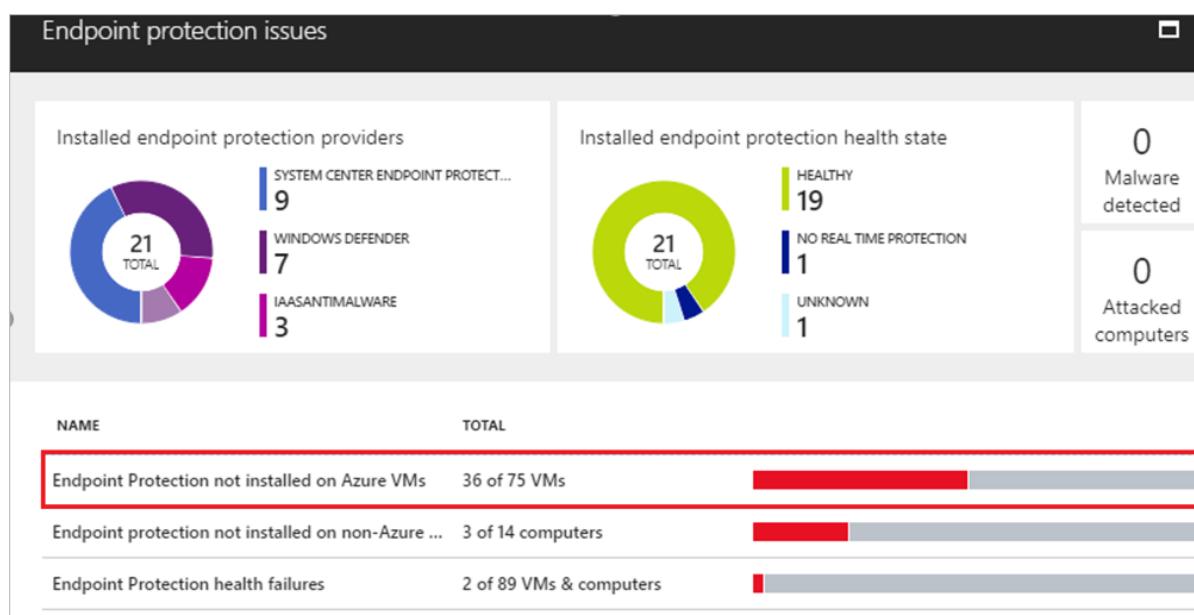


Figure 1: Antimalware for VMs.

## Learn more:

- Learn about [Microsoft Antimalware for Azure](#).

## Best practice: Secure web apps

Migrated web apps face a couple of issues:

- Most legacy web applications tend to have sensitive information inside configuration files. Files containing such information can present security issues when applications are backed up, or when application code is checked into or out of source control.
- When you migrate web apps residing in a VM, you're likely moving that machine from an on-premises network and firewall-protected environment, to an environment facing the internet. Make sure that you set up a solution that does the same work as your on-premises protection resources.

Azure provides the following solutions:

- **Azure Key Vault:** Today, web app developers are taking steps to ensure that sensitive information isn't leaked from these files. One method to secure information is to extract it from files and put it into an Azure Key Vault.
  - You can use Key Vault to centralize storage of application secrets, and control their distribution. It avoids the need to store security information in application files.
  - Applications can securely access information in the vault by using URLs, without needing custom code.
  - Azure Key Vault allows you to lock down access via Azure security controls, and to seamlessly implement rolling keys. Microsoft doesn't see or extract your data.
- **App Service Environment for Power Apps:** If an application that you migrate needs extra protection, consider adding App Service Environment and Web Application Firewall to protect the application resources.
  - App Service Environment provides a fully isolated and dedicated environment for running applications, such as Windows and Linux web apps, Docker containers, mobile apps, and function apps.
  - It's useful for applications that are very high scale, require isolation and secure network access, or have high memory utilization.
- **Web Application Firewall:** This is a feature of Azure Application Gateway that provides centralized protection for web apps.
  - It protects web apps without requiring back-end code modifications.
  - It protects multiple web apps at the same time, behind Application Gateway.
  - You can monitor Web Application Firewall by using Azure Monitor. Web Application Firewall is integrated into Azure Security Center.

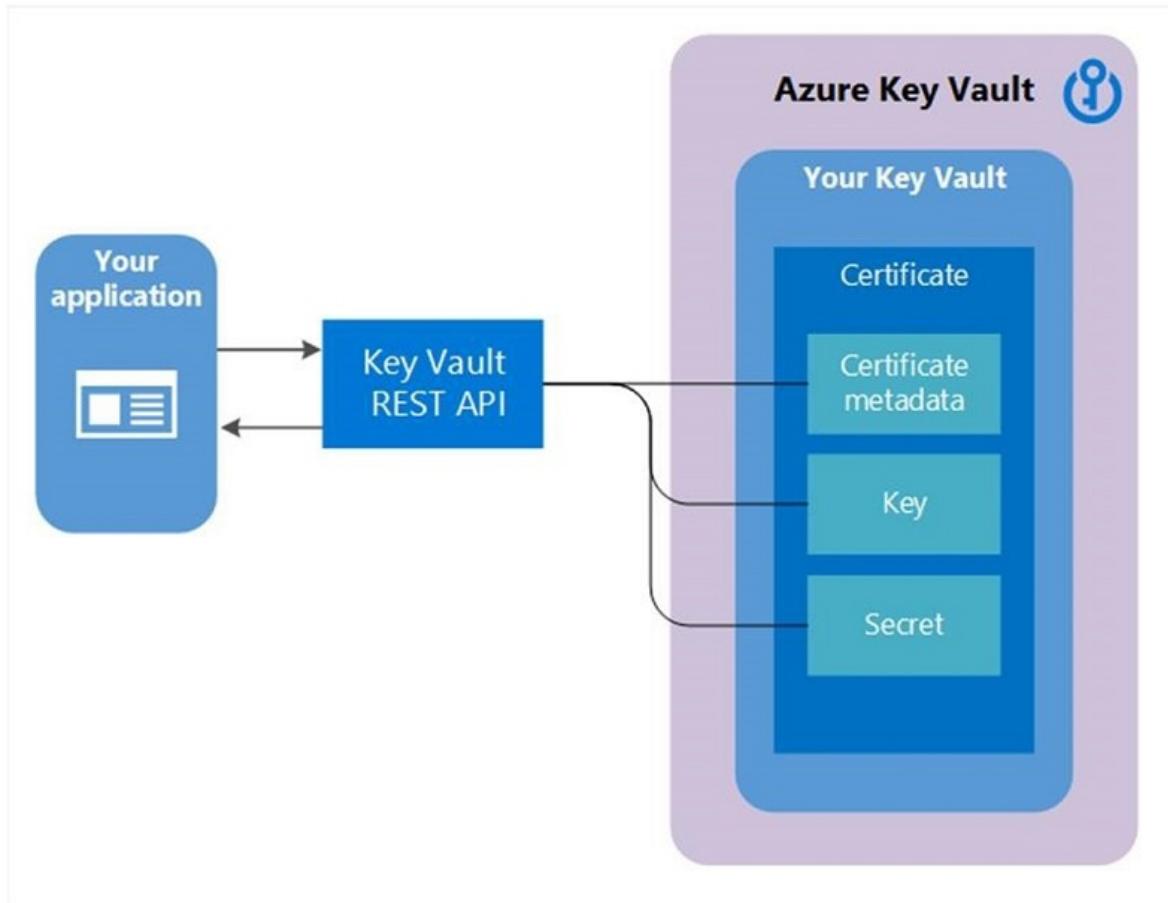


Figure 2: Azure Key Vault.

#### Learn more:

- Read the [Azure Key Vault overview](#).
- Learn about [Web Application Firewall](#).
- Read an [introduction to App Service environments](#).
- Learn how to [configure a web app to read secrets from Key Vault](#).

## Best practice: Review subscriptions and resource permissions

As you migrate your workloads and run them in Azure, staff with workload access move around. Your security team should review access to your Azure tenant and resource groups on a regular basis. Azure has offerings for identity management and access control security, including role-based access control (RBAC) to authorize permissions to access Azure resources.

- RBAC assigns access permissions for security principals. Security principals represent users, groups (a set of users), service principals (identity used by applications and services), and managed identities (an Azure Active Directory identity automatically managed by Azure).
- RBAC can assign roles to security principals, such as owner, contributor and reader, and role definitions (a collection of permissions) that define the operations that can be performed by the roles.
- RBAC can also set scopes that set the boundary for a role. Scope can be set at several levels, including a management group, subscription, resource group, or resource.
- Ensure that admins with Azure access can access only resources that you want to allow. If the predefined roles in Azure aren't granular enough, you can create custom roles to separate and limit access permissions.

Ensure that admins with Azure access can access only resources that you want to allow. If the predefined roles in Azure aren't granular enough, you can create custom roles to separate and limit access permissions.

The screenshot shows the Microsoft Azure portal interface. The left sidebar contains a navigation menu with options like 'Create a resource', 'All services', 'FAVORITES' (Dashboard, All resources, Resource groups, App Services, Function Apps, SQL databases, Azure Cosmos DB, Virtual machines, Load balancers, Storage accounts, Virtual networks, Azure Active Directory), and 'COST MANAGEMENT + BILLING' (Invoices, Cost analysis, External services, Payment methods, Partner information). The main content area is titled 'Pay-As-You-Go - Access control (IAM)' and shows an 'Overview' section with a search bar and filters for 'Name', 'Type', 'Scope', and 'Role'. A table lists three items: a group named 'Billing Reader' (PS Pharma Sales ... Group, Billing Reader role, This resource), an owner named 'Robert' (RL Robert User, Owner role, Service admin..., This resource), and a reader named 'App2' (App2 App, Reader role, This resource).

Figure 3: Access control.

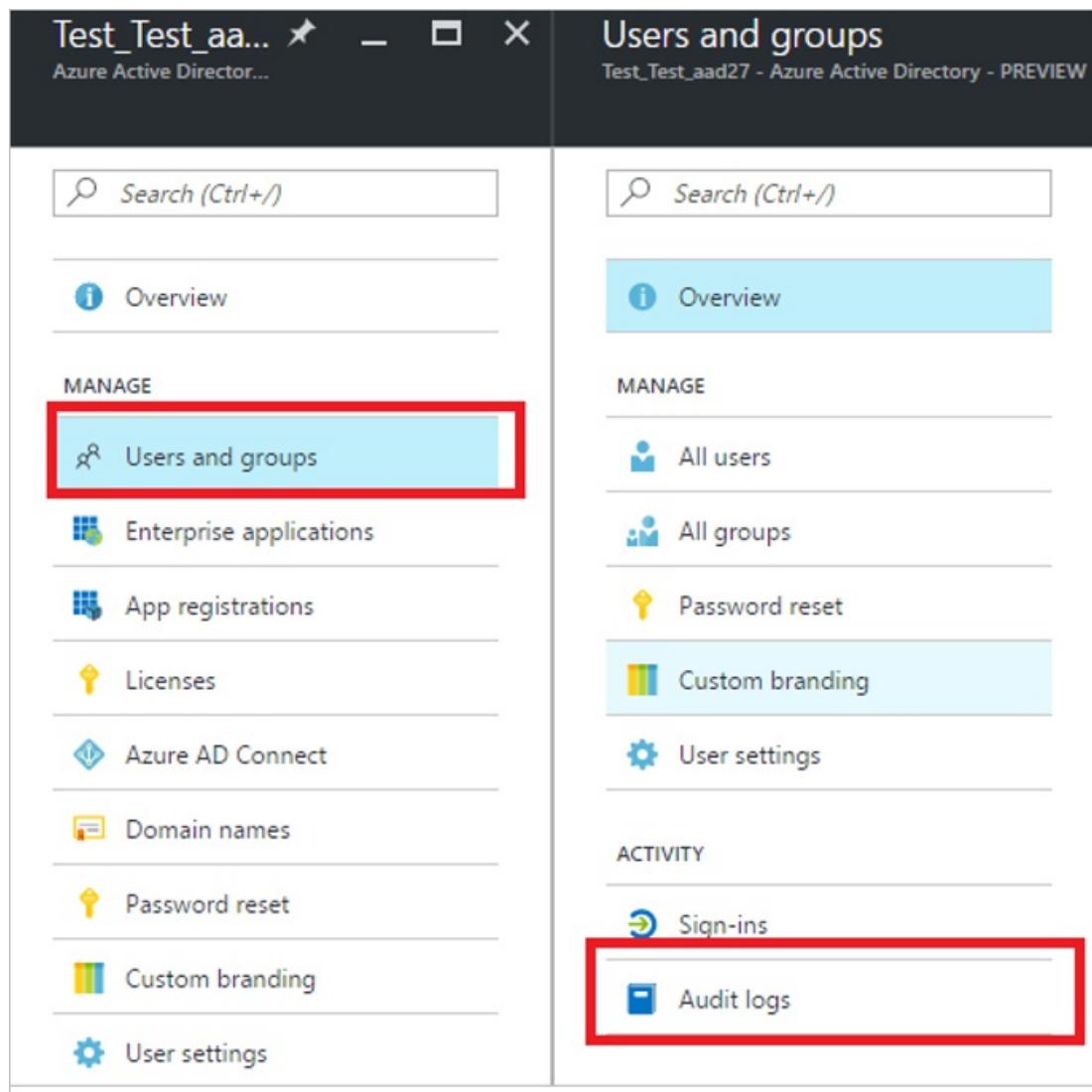
#### Learn more:

- Learn about [Azure role-based access control \(RBAC\)](#).
- Learn to manage access via [RBAC and the Azure portal](#).
- Learn about [custom roles](#).

## Best practice: Review audit and security logs

Azure Active Directory (Azure AD) provides activity logs that appear in Azure Monitor. The logs capture the operations performed in Azure tenancy, when they occurred, and who performed them.

- Audit logs show the history of tasks in the tenant. Sign-in activity logs show who carried out the tasks.
- Access to security reports depends on your Azure AD license. With the free and basic licenses, you get a list of risky users and sign-ins. With the premium licenses, you get underlying event information.
- You can route activity logs to various endpoints for long-term retention and data insights.
- Make it a common practice to review the logs, or integrate your security information and event management (SIEM) tools to automatically review abnormalities. If you're not using a premium license, you'll need to do a lot of analysis yourself, or by using your SIEM system. Analysis includes looking for risky sign-ins and events, and other user attack patterns.



Figure

4: Azure AD users and groups.

#### Learn more:

- Learn about [Azure AD activity logs in Azure Monitor](#).
- Learn how to [audit activity reports in the Azure AD portal](#).

## Best practice: Evaluate other security features

Azure provides other security features that provide advanced security options. Note that some of the following best practices require add-on licenses and premium options.

- **Implement Azure AD administrative units (AU).** Delegating administrative duties to support staff can be tricky with just basic Azure access control. Giving support staff access to administer all the groups in Azure AD might not be the ideal approach for organizational security. Using AU allows you to segregate Azure resources into containers in a similar way to on-premises organizational units (OU). To use AU, the AU admin must have a premium Azure AD license. For more information, see [Administrative units management in Azure Active Directory](#).
- **Use multi-factor authentication.** If you have a premium Azure AD license, you can enable and enforce multi-factor authentication on your admin accounts. Phishing is the most common way that accounts credentials are compromised. When a bad actor has admin account credentials, there's no stopping them from far-reaching actions, such as deleting all of your resource groups. You can establish multi-factor authentication in several ways, including with email, an authenticator app, and phone text messages. As an administrator, you can select the least intrusive option. Multi-factor authentication integrates with threat analytics and conditional access policies to randomly require a multi-factor authentication challenge response. Learn more about [security](#)

[guidance](#), and [how to set up multi-factor authentication](#).

- **Implement conditional access.** In most small and medium-sized organizations, Azure admins and the support team are probably located in a single geography. In this case, most sign-ins come from the same areas. If the IP addresses of these locations are fairly static, it makes sense that you shouldn't see administrator sign-ins from outside these areas. Even if a remote bad actor compromises an administrator's credentials, you can implement security features like conditional access, combined with multi-factor authentication, to prevent signing in from remote locations. This can also prevent spoofed locations from random IP addresses. Learn more about [conditional access](#) and [review best practices](#) for conditional access in Azure AD.
- **Review enterprise application permissions.** Over time, admins select Microsoft and third-party links without knowing their affect on the organization. Links can present consent screens that assign permissions to Azure apps. This might allow access to read Azure AD data, or even full access to manage your entire Azure subscription. You should regularly review the applications to which your admins and users have allowed access to Azure resources. Ensure that these applications have only the permissions that are necessary. Additionally, quarterly or semi-annually you can email users with a link to application pages, so that they're aware of the applications to which they've allowed access to their organizational data. For more information, see [Unexpected application in my applications list](#), and [how to control](#) application assignments in Azure AD.

## Managed migrated workloads

In the following sections, we'll recommend some best practices for Azure management, including:

- Best practices for Azure resource groups and resources, including smart naming, preventing accidental deletion, managing resource permissions, and effective resource tagging.
- Get a quick overview on using blueprints for building and managing your deployment environments.
- Review sample Azure architectures to learn from as you build your post-migration deployments.
- If you have multiple subscriptions, you can gather them into management groups, and apply governance settings to those groups.
- Apply compliance policies to your Azure resources.
- Put together a business continuity and disaster recovery (BCDR) strategy to keep data safe, your environment resilient, and resources up and running when outages occur.
- Group VMs into availability groups for resilience and high availability. Use managed disks for ease of VM disk and storage management.
- Enable diagnostic logging for Azure resources, build alerts and playbooks for proactive troubleshooting, and use the Azure dashboard for a unified view of your deployment health and status.
- Understand your Azure support plan and how to implement it, get best practices for keeping VMs up-to-date, and put processes in place for change management.

## Best practice: Name resource groups

Ensure that your resource groups have meaningful names that admins and support team members can easily recognize and scan. This can drastically improve productivity and efficiency.

If you're synchronizing your on-premises Active Directory to Azure AD by using Azure AD Connect, consider matching the names of security groups on-premises to the names of resource groups in Azure.

The screenshot displays two windows side-by-side. The top window is the 'Resource groups' blade in the Azure portal, titled 'Contoso Migration'. It shows a list of resource groups under the 'contoso' subscription. The bottom window is the 'Active Directory Administrative Center' showing the 'ContosoGroups' list for the 'contoso (local)' domain. Both lists include the same resource groups: ContosoCobRG, ContosoDevRG, ContosoFailoverRG, ContosoInfraRG, ContosoNetworkingRG, and ContosoRG.

Name	Type	Description
ContosoAzureAdmins	Group	Azure Resource Group
ContosoCobRG	Group	Azure Resource Group
ContosoDevRG	Group	Azure Resource Group
ContosoFailoverRG	Group	Azure Resource Group
ContosoInfraRG	Group	Azure Resource Group
ContosoNetworkingRG	Group	Azure Resource Group
ContosoRG	Group	Azure Resource Group

*Figure 5: Resource group naming.*

#### Learn more:

- Learn about [recommended naming conventions](#).

## Best practice: Implement delete locks for resource groups

The last thing you need is for a resource group to disappear because it was deleted accidentally. We recommend that you implement delete locks, so that this doesn't happen.

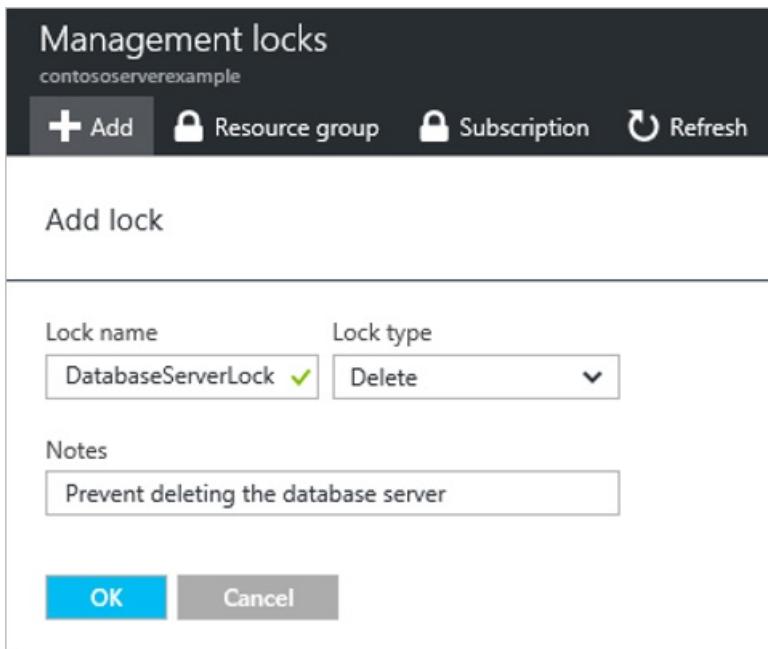


Figure 6: Delete locks.

**Learn more:**

- Learn about [locking resources to prevent unexpected changes](#).

## Best practice: Understand resource access permissions

A subscription owner has access to all the resource groups and resources in your subscription.

- Add people sparingly to this valuable assignment. Understanding the ramifications of these types of permissions is important in keeping your environment secure and stable.
- Make sure you place resources in appropriate resources groups:
  - Match resources with a similar lifecycle together. Ideally, you shouldn't need to move a resource when you need to delete an entire resource group.
  - Resources that support a function or workload should be placed together for simplified management.

**Learn more:**

- Learn about [organizing subscriptions and resource groups](#).

## Best practice: Tag resources effectively

Often, using only a resource group name related to resources won't provide enough metadata for effective implementation of mechanisms, such as internal billing or management within a subscription.

- As a best practice, use Azure tags to add useful metadata that can be queried and reported on.
- Tags provide a way to logically organize resources with properties that you define. Tags can be applied to resource groups or resources directly.
- Tags can be applied on a resource group or on individual resources. Resource group tags aren't inherited by the resources in the group.
- You can automate tagging by using PowerShell or Azure Automation, or tag individual groups and resources.
- If you have a request and change management system in place, then you can easily use the information in the request to populate your company-specific resource tags.

The screenshot shows the Azure portal interface for a resource group named 'demoGroup'. On the left, there's a sidebar with options like 'Overview', 'Activity log', 'Access control (IAM)', and 'Tags'. The main area shows a table with columns for 'Subscription (change)' and 'Subscription ID'. A red box highlights the 'Tags (change)' section, which contains two entries: 'Dept : Finance' and 'Environment : Production'. There are also buttons for 'Edit columns' and 'Delete resource group'.

Figure 7: Tagging.

#### Learn more:

- Learn about [tagging and tag limitations](#).
- Review [PowerShell and CLI examples to set up tagging, and to apply tags from a resource group to its resources](#).
- [Read Azure tagging best practices](#).

## Best practice: Implement blueprints

Just as a blueprint allows engineers and architects to sketch a project's design parameters, the Azure Blueprints service enables cloud architects and central IT groups to define a repeatable set of Azure resources. This helps them to implement and adhere to an organization's standards, patterns, and requirements. Using Azure Blueprints, development teams can rapidly build and create new environments that meet organizational compliance requirements. These new environments have a set of built-in components, such as networking, to speed up development and delivery.

- Use blueprints to orchestrate the deployment of resource groups, Azure Resource Manager templates, and policy and role assignments.
- Store blueprints in a globally distributed service, Azure Cosmos DB. Blueprint objects are replicated to multiple Azure regions. Replication provides low latency, high availability, and consistent access to a blueprint, regardless of the region to which a blueprint deploys resources.

#### Learn more:

- [Read about blueprints](#).
- Review an [example blueprint for accelerating AI in healthcare](#).

## Best practice: Review Azure reference architectures

Building secure, scalable, and manageable workloads in Azure can be daunting. With continual changes, it can be difficult to keep up with different features for an optimal environment. Having a reference to learn from can be helpful when designing and migrating your workloads. Azure and Azure partners have built several sample reference architectures for various types of environments. These samples are designed to provide ideas that you can learn from and build on.

Reference architectures are arranged by scenario. They contain best practices and advice on management, availability, scalability, and security. App Service Environment provides a fully isolated and dedicated environment for running applications, such as Windows and Linux web apps, Docker containers, mobile apps, and functions. App Service adds the power of Azure to your application, with security, load balancing, autoscaling, and automated management. You can also take advantage of its DevOps capabilities, such as continuous deployment from Azure

DevOps and GitHub, package management, staging environments, custom domain, and SSL certificates. App Service is useful for applications that need isolation and secure network access, and those that use high amounts of memory and other resources that need to scale.

#### Learn more:

- Learn about [Azure reference architectures](#).
- Review [Azure example scenarios](#).

## Best practice: Manage resources with Azure management groups

If your organization has multiple subscriptions, you need to manage access, policies, and compliance for them. Azure management groups provide a level of scope above subscriptions. Here are some tips:

- You organize subscriptions into containers called management groups, and apply governance conditions to them.
- All subscriptions in a management group automatically inherit the management group conditions.
- Management groups provide large-scale, enterprise-grade management, no matter what type of subscriptions you have.
- For example, you can apply a management group policy that limits the regions in which VMs can be created. This policy is then applied to all management groups, subscriptions, and resources under that management group.
- You can build a flexible structure of management groups and subscriptions, to organize your resources into a hierarchy for unified policy and access management.

The following diagram shows an example of creating a hierarchy for governance by using management groups.

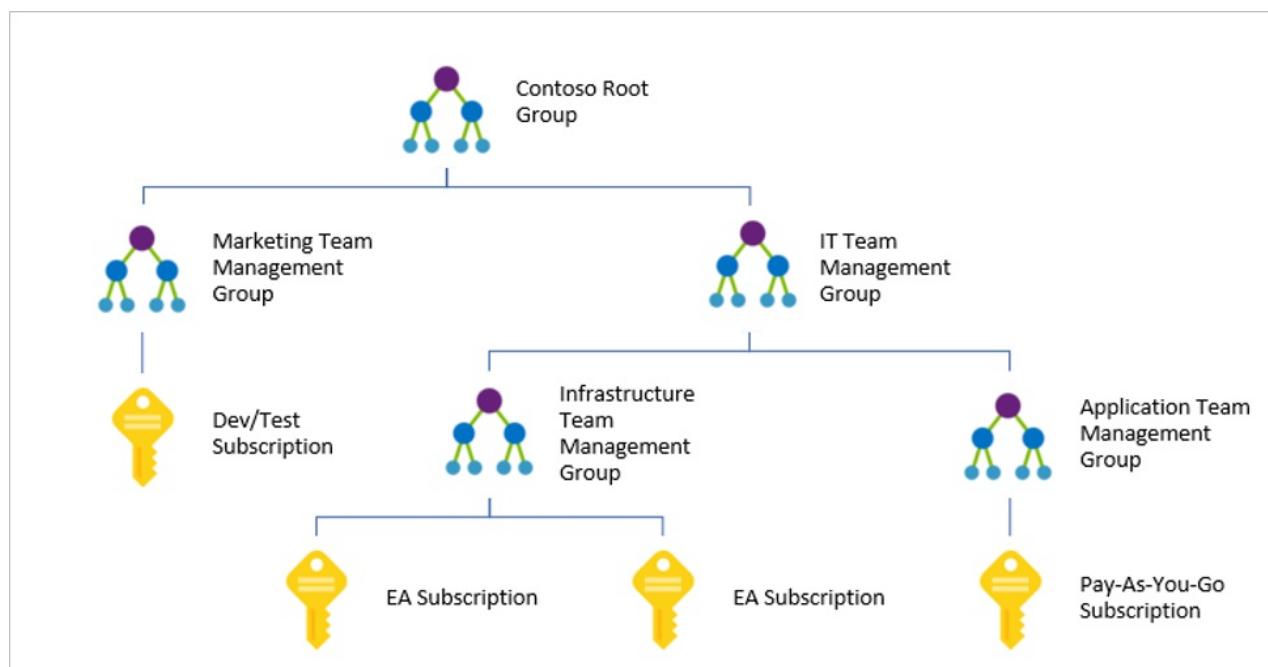


Figure 8: Management groups.

#### Learn more:

- Learn more about [organizing resources into management groups](#).

## Best practice: Deploy Azure Policy

Azure Policy is a service that you use to create, assign, and manage policies. Policies enforce different rules and effects over your resources, so those resources stay compliant with your corporate standards and service-level agreements.

Azure Policy evaluates your resources, scanning for those not compliant with your policies. For example, you can create a policy that allows only a specific SKU size for VMs in your environment. Azure Policy will evaluate this setting when you create and update resources, and when scanning existing resources. Note that Azure provides some built-in policies that you can assign, or you can create your own.

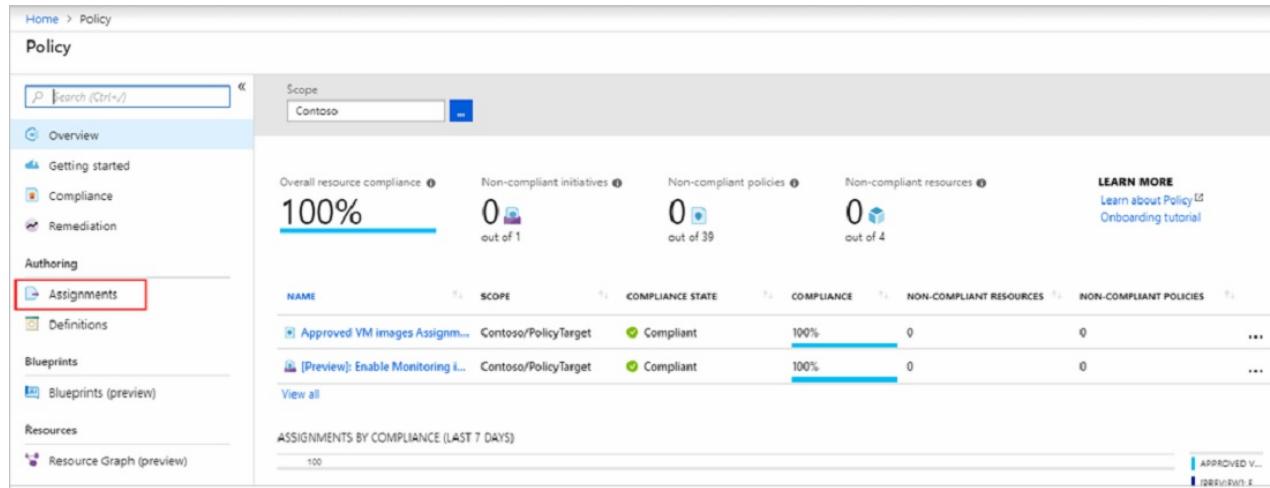


Figure 9: Azure Policy.

#### Learn more:

- Read the [Azure Policy overview](#).
- Learn about [creating and managing policies to enforce compliance](#).

## Best practice: Implement a BCDR strategy

Planning for business continuity and disaster recovery (BCDR) is a critical exercise that you should complete as part of your Azure migration planning process. In legal terms, your contracts might include a *force majeure* clause that excuses obligations due to a greater force, such as hurricanes or earthquakes. But you also have obligations around your ability to ensure that services will continue to run, and recover where necessary, when disaster strikes. Your ability to do this can make or break your company's future.

Broadly, your BCDR strategy must consider:

- **Data backup:** How to keep your data safe so that you can recover it easily if outages occur.
- **Disaster recovery:** How to keep your applications resilient and available if outages occur.

#### Set up BCDR

When migrating to Azure, understand that although the Azure platform provides some built-in resiliency capabilities, you need to design your Azure deployment to take advantage of them.

- Your BCDR solution will depend on your company objectives, and is influenced by your Azure deployment strategy. Infrastructure as a service (IaaS) and platform as a service (PaaS) deployments present different challenges for BCDR.
- After they are in place, your BCDR solutions should be tested regularly to check that your strategy remains viable.

#### Back up an IaaS deployment

In most cases, an on-premises workload is retired after migration, and your on-premises strategy for backing up data must be extended or replaced. If you migrate your entire datacenter to Azure, you'll need to design and implement a full backup solution by using Azure technologies, or third-party integrated solutions.

For workloads running on Azure IaaS VMs, consider these backup solutions:

- **Azure Backup:** Provides application-consistent backups for Azure Windows and Linux VMs.

- **Storage snapshots:** Takes snapshots of Blob storage.

#### Azure Backup

Azure Backup creates data recovery points that are stored in Azure Storage. Azure Backup can back up Azure VM disks, and Azure Files (preview). Azure Files provide file shares in the cloud, accessible via Server Message Block.

You can use Azure Backup to back up VMs in the following ways:

- **Direct backup from VM settings.** You can back up VMs with Azure Backup directly from the VM options in the Azure portal. You can back up the VM once per day, and you can restore the VM disk as needed. Azure Backup takes app-aware data snapshots, and no agent is installed on the VM.
- **Direct backup in a Recovery Services vault.** You can back up your IaaS VMs by deploying an Azure Backup Recovery Services vault. This provides a single location to track and manage backups, as well as granular backup and restore options. Backup is up to three times a day, at the file and folder levels. It isn't app-aware, and Linux isn't supported. Install the Microsoft Azure Recovery Services (MARS) agent on each VM that you want to back up by using this method.
- **Protect the VM to Azure Backup server.** Azure Backup server is provided free with Azure Backup. The VM is backed up to local Azure Backup server storage. You then back up the Azure Backup server to Azure in a vault. Backup is app-aware, with full granularity over backup frequency and retention. You can back up at the application level, for example by backing up SQL Server or SharePoint.

For security, Azure Backup encrypts data in-flight by using AES-256. It sends it over HTTPS to Azure. Backed-up data-at-rest in Azure is encrypted by using [Azure Storage encryption](#).

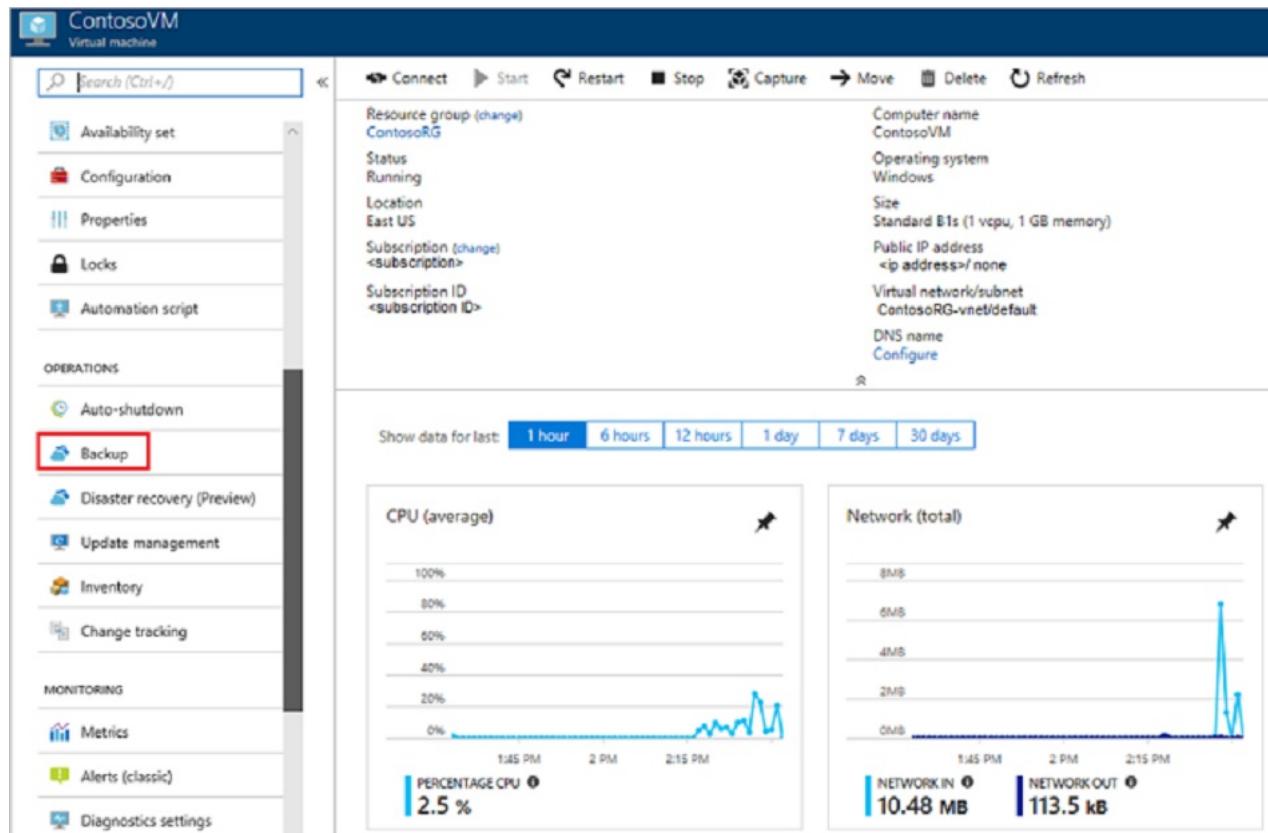


Figure 10: Azure Backup.

#### Learn more:

- Learn about [Azure Backup](#).
- Plan a [backup infrastructure for Azure VMs](#).

#### Storage snapshots

Azure VMs are stored as page blobs in Azure Storage. Snapshots capture the blob state at a specific point in time. As an alternative backup method for Azure VM disks, you can take a snapshot of storage blobs and copy them to

another storage account.

You can copy an entire blob, or use an incremental snapshot copy to copy only delta changes and reduce storage space. As an extra precaution, you can enable soft delete for Blob storage accounts. With this feature enabled, a blob that's deleted is marked for deletion, but not immediately purged. During the interim period, you can restore the blob.

#### Learn more:

- Learn about [Azure Blob storage](#).
- Learn how to [create a blob snapshot](#).
- [Review a sample scenario](#) for Blob storage backup.
- Read about [soft delete for blobs](#).
- [Disaster recovery and forced failover \(preview\) in Azure Storage](#)

#### Third-party backup

In addition, you can use third-party solutions to back up Azure VMs and storage containers to local storage or other cloud providers. For more information, see [Backup solutions in Azure Marketplace](#).

#### Set up disaster recovery for IaaS applications

In addition to protecting data, BCDR planning must consider how to keep applications and workloads available if a disaster occurs. For workloads that run on Azure IaaS VMs and Azure Storage, consider the solutions in the following sections.

##### Azure Site Recovery

Azure Site Recovery is the primary Azure service for ensuring that Azure VMs can be brought online, and VM applications made available, when outages occur.

Site Recovery replicates VMs from a primary to a secondary Azure region. If disaster strikes, you fail VMs over from the primary region, and continue accessing them as normal in the secondary region. When operations return to normal, you can fail back VMs to the primary region.

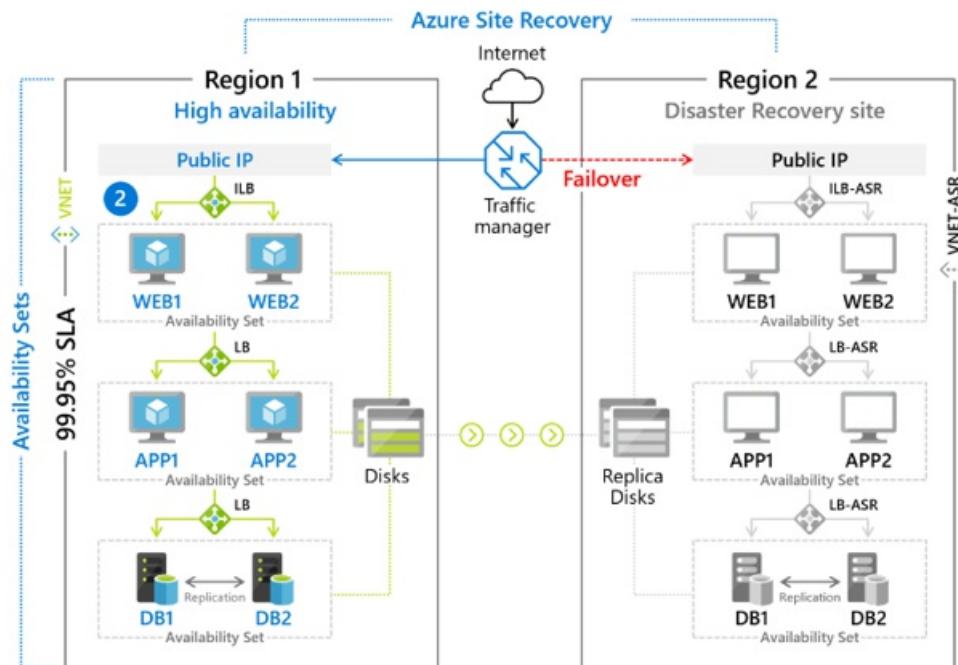


Figure 11: Site Recovery.

#### Learn more:

- Review [disaster recovery scenarios for Azure VMs](#).
- Learn how to [set up disaster recovery for an Azure VM after migration](#).

## Best practice: Use managed disks and availability sets

Azure uses availability sets to logically group VMs together, and to isolate VMs in a set from other resources. VMs in an availability set are spread across multiple fault domains with separate subsystems, which protects against local failures. The VMs are also spread across multiple update domains, preventing a simultaneous reboot of all VMs in the set.

Azure managed disks simplify disk management for Azure Virtual Machines by managing the storage accounts associated with the VM disks.

- Use managed disks wherever possible. You only have to specify the type of storage you want to use and the size of disk you need, and Azure creates and manages the disk for you.
- You can convert existing disks to managed disks.
- You should create VMs in availability sets for high resilience and availability. When planned or unplanned outages occur, availability sets ensure that at least one VM in the set remains available.

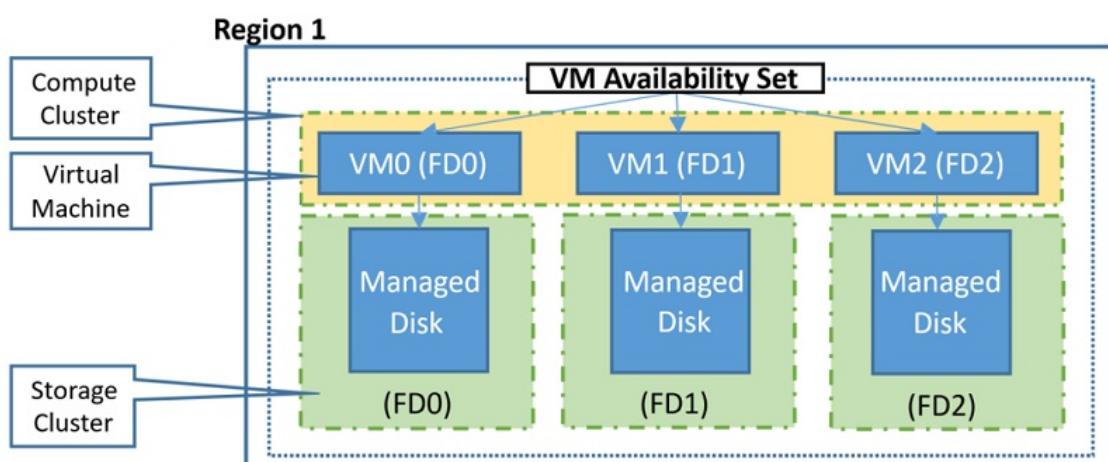


Figure 12: Managed disks.

### Learn more:

- Read the [managed disks overview](#).
- Learn about [converting disks to managed](#).
- Learn how to [manage the availability of Windows VMs in Azure](#).

## Best practice: Monitor resource usage and performance

You might have moved your workloads to Azure for its immense scaling capabilities. But moving your workload doesn't mean that Azure will automatically implement scaling without your input. Here are two examples:

- If your marketing organization pushes a new television advertisement that drives 300 percent more traffic, this might cause site availability issues. Your newly migrated workload might hit assigned limits, and crash.
- If there's a distributed denial-of-service (DDoS) attack on your migrated workload, in this case you don't want to scale. You want to prevent the source of the attacks from reaching your resources.

These two cases have different resolutions, but for both you need insight into what's happening with usage and performance monitoring.

- Azure Monitor can help surface these metrics, and provide response with alerts, autoscaling, event hubs, and logic apps.
- You can also integrate your third-party SIEM application to monitor the Azure logs for auditing and

performance events.

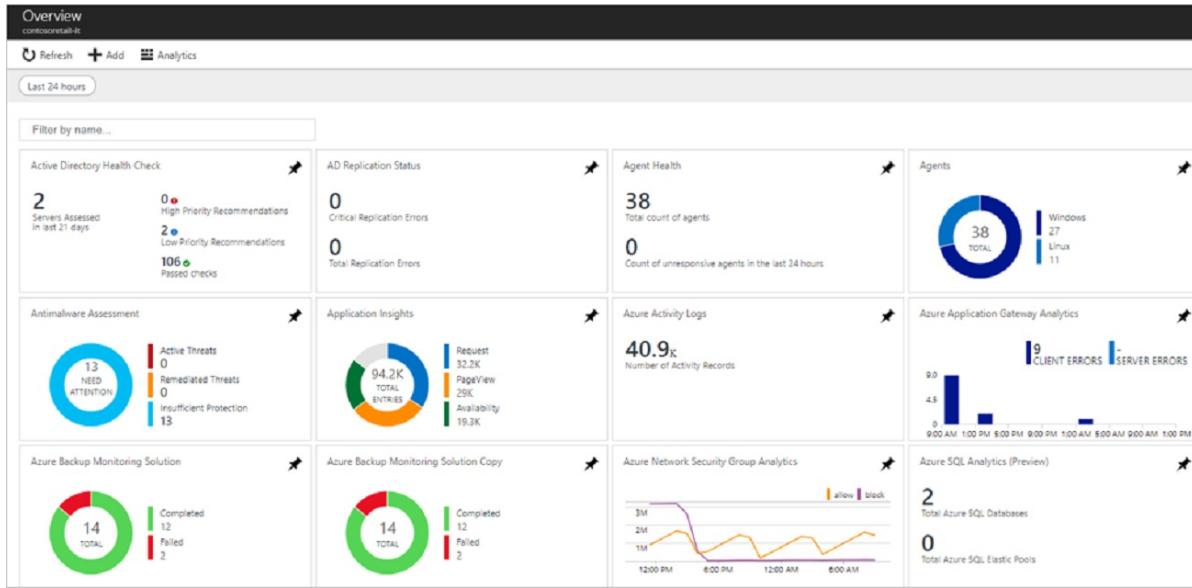


Figure 13: Azure Monitor.

#### Learn more:

- Learn about [Azure Monitor](#).
- [Get best practices](#) for monitoring and diagnostics.
- Learn about [autoscaling](#).
- Learn how to [route Azure data to a SIEM tool](#).

## Best practice: Enable diagnostic logging

Azure resources generate a fair number of logging metrics and telemetry data. By default, most resource types don't have diagnostic logging enabled. By enabling diagnostic logging across your resources, you can query logging data, and build alerts and playbooks based on it.

When you enable diagnostic logging, each resource will have a specific set of categories. You select one or more logging categories, and a location for the log data. Logs can be sent to a storage account, event hub, or to Azure Monitor logs.

The screenshot shows the 'Diagnostics settings' section of the Azure Monitor. On the left, there's a sidebar with links like Metrics, Log Analytics, Activity log, Service Health, Application Insights, Network watcher, Management solutions, and a selected 'Diagnostics settings'. The main area has a 'Refresh' button and filters for Subscription (Azure Monitor Demo), Resource group (ContosoLoanApp1), Resource type (7 selected), and a search bar. Below this, a message says 'Select any of the resources to view logs.' A table lists 10 resources with their names, resource types, resource groups, and diagnostics status (all enabled). The resources include Event Hubs, Logic apps, Load balancers, and Network security groups.

NAME	RESOURCE TYPE	RESOURCE GROUP	DIAGNOSTICS STATUS
loanprocessingEH	Event Hub	ContosoLoanApp1	Enabled
routetooELK1	Event Hub	ContosoLoanApp1	Enabled
LoanAppLA	Logic app	ContosoLoanApp1	Enabled
mvpsummitLogicApp1	Logic app	ContosoLoanApp1	Enabled
simplealerttest1	Logic app	ContosoLoanApp1	Enabled
simpletest2	Logic app	ContosoLoanApp1	Enabled
bizdkscvklb	Load balancer	ContosoLoanApp1	Enabled
loanprocklb	Load balancer	ContosoLoanApp1	Enabled
loandatabasevm2-nsg	Network security group	ContosoLoanApp1	Enabled
loandatabasevm1-nsg	Network security group	ContosoLoanApp1	Enabled

Figure 14: Diagnostic logging.

#### Learn more:

- Learn about [collecting and consuming log data](#).
- Learn what's supported for [diagnostic logging](#).

## Best practice: Set up alerts and playbooks

With diagnostic logging enabled for Azure resources, you can start to use logging data to create custom alerts.

- Alerts proactively notify you when conditions are found in your monitoring data. You can then address issues before system users notice them. You can alert on metric values, log search queries, activity log events, platform health, and website availability.
- When alerts are triggered, you can run a logic app playbook. A playbook helps you to automate and orchestrate a response to a specific alert. Playbooks are based on Azure Logic Apps. You can use logic app templates to create playbooks, or create your own.
- As a simple example, you can create an alert that triggers when a port scan happens against a network security group. You can set up a playbook that runs and locks down the IP address of the scan origin.
- Another example is an application with a memory leak. When the memory usage gets to a certain point, a playbook can recycle the process.

The screenshot shows the 'Alerts' dashboard. At the top, it displays 'Total Alerts' (2612), 'Smart Groups' (78), and 'Total Alert Rules' (285). It also shows a 'Time Range' of 'Past 24 Hours'. Below this, there's a summary table with columns for Severity, Total Alerts, New, Acknowledged, and Closed. The severity categories are Sev 0, Sev 1, Sev 2, Sev 3, and Sev 4. The table shows the count of alerts for each severity level and the status of those alerts.

SEVERITY	TOTAL ALERTS	NEW	ACKNOWLEDGED	CLOSED
Sev 0	267	287	0	0
Sev 1	598	598	0	0
Sev 2	59	59	0	0
Sev 3	1494	1494	0	0
Sev 4	174	174	0	0

Figure 15: Alerts.

## Learn more:

- Learn about [alerts](#).
- Learn about [security playbooks that respond to Security Center alerts](#).

## Best practice: Use the Azure dashboard

The Azure portal is a web-based unified console that allows you to build, manage, and monitor everything from simple web apps to complex cloud applications. It includes a customizable dashboard and accessibility options.

- You can create multiple dashboards, and share them with others who have access to your Azure subscriptions.
- With this shared model, your team has visibility into the Azure environment, allowing them to be proactive when managing systems in the cloud.

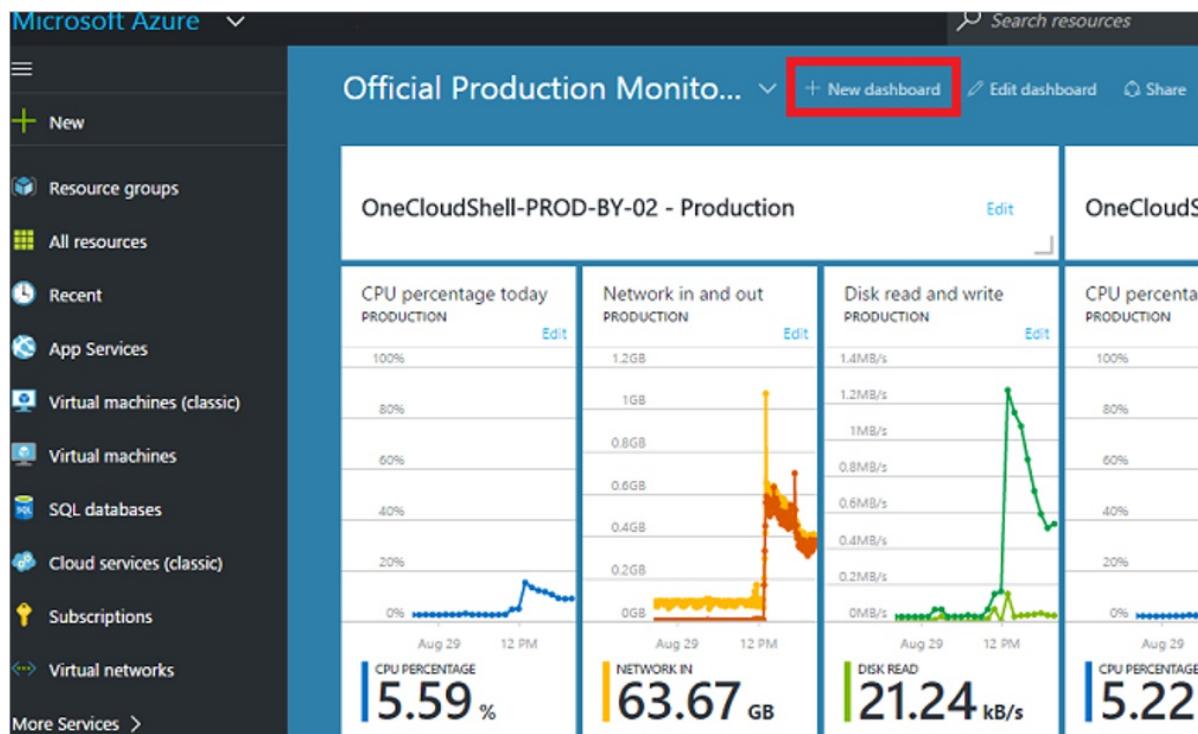


Figure 16: Azure dashboard.

## Learn more:

- Learn how to [create a dashboard](#).
- Learn about [dashboard structure](#).

## Best practice: Understand support plans

At some point, you will need to collaborate with your support staff or Microsoft support staff. Having a set of policies and procedures for support during scenarios such as disaster recovery is vital. In addition, your admins and support staff should be trained on implementing those policies.

- In the unlikely event that an Azure service issue affects your workload, admins should know how to submit a support ticket to Microsoft in the most appropriate and efficient way.
- Familiarize yourself with the various support plans offered for Azure. They range from response times dedicated to developer instances, to premier support with a response time of less than 15 minutes.

	BASIC	DEVELOPER	STANDARD	PROFESSIONAL DIRECT	Premier
	Purchase support	Purchase support	Purchase support	Purchase support	Contact Premier
Case Severity/Response Times	Minimal business impact (Sev C): <8 business hours <sup>1</sup>	Minimal business impact (Sev C): <8 business hours <sup>1</sup> Moderate business impact (Sev B): <4 hours Critical business impact (Sev A): <1 hour	Minimal business impact (Sev C): <4 business hours <sup>1</sup> Moderate business impact (Sev B): <2 hours Critical business impact (Sev A): <1 hour	Minimal business impact (Sev C): <4 business hours <sup>1</sup> Moderate business impact (Sev B): <2 hours Critical business impact (Sev A): <1 hour	Minimal business impact (Sev C): <4 business hours <sup>1</sup> Moderate business impact (Sev B): <2 hours Critical business impact (Sev A): <1 hour <15 minutes (with Azure Rapid Response or Azure Event Management)

Figure 17: Support plans.

#### Learn more:

- Read an [overview of Azure support plans](#).
- Learn about [service-level agreements \(SLAs\)](#).

## Best practice: Manage updates

Keeping Azure VMs updated with the latest operating system and software updates is a massive chore. The ability to surface all VMs, figure out which updates they need, and automatically push those updates is extremely valuable.

- You can use update management in Azure Automation to manage operating system updates. This applies to machines that run Windows and Linux computers that are deployed in Azure, on-premises, and in other cloud providers.
- Use update management to quickly assess the status of available updates on all agent computers, and manage update installation.
- You can enable update management for VMs directly from an Azure Automation account. You can also update a single VM from the VM page in the Azure portal.
- In addition, you can register Azure VMs with System Center Configuration Manager. You can then migrate the Configuration Manager workload to Azure, and do reporting and software updates from a single web interface.

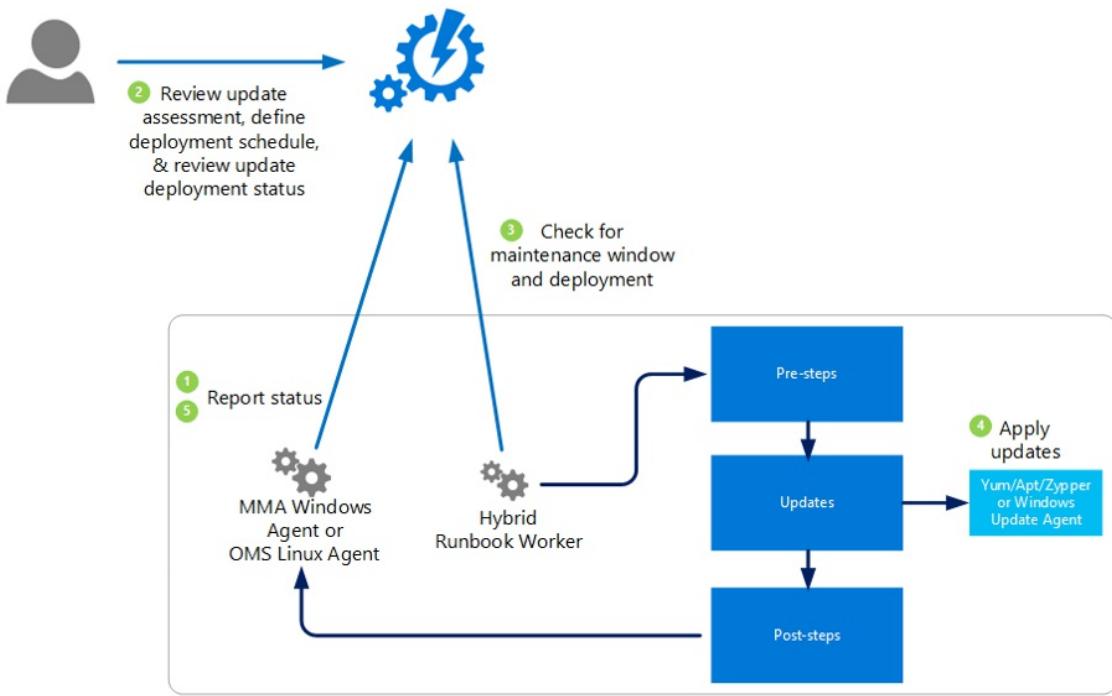


Figure 18: Updates.

#### Learn more:

- Learn about [update management in Azure](#).
- Learn how to [integrate Configuration Manager with update management](#).
- [Frequently asked questions](#) about Configuration Manager in Azure.

## Implement a change management process

As with any production system, making any type of change can affect your environment. A change management process that requires requests to be submitted in order to make changes to production systems is a valuable addition in your migrated environment.

- You can build best practice frameworks for change management to raise awareness in administrators and support staff.
- You can use Azure Automation to help with configuration management and change tracking for your migrated workflows.
- When enforcing change management process, you can use audit logs to link Azure change logs to existing change requests. Then, if you see a change made without a corresponding change request, you can investigate what went wrong in the process.

Azure has a change-tracking solution in Azure Automation:

- The solution tracks changes to Windows and Linux software and files, Windows registry keys, Windows services, and Linux daemons.
- Changes on monitored servers are sent to Azure Monitor for processing.
- Logic is applied to the received data, and the cloud service records the data.
- On the change tracking dashboard, you can easily see the changes that were made in your server infrastructure.

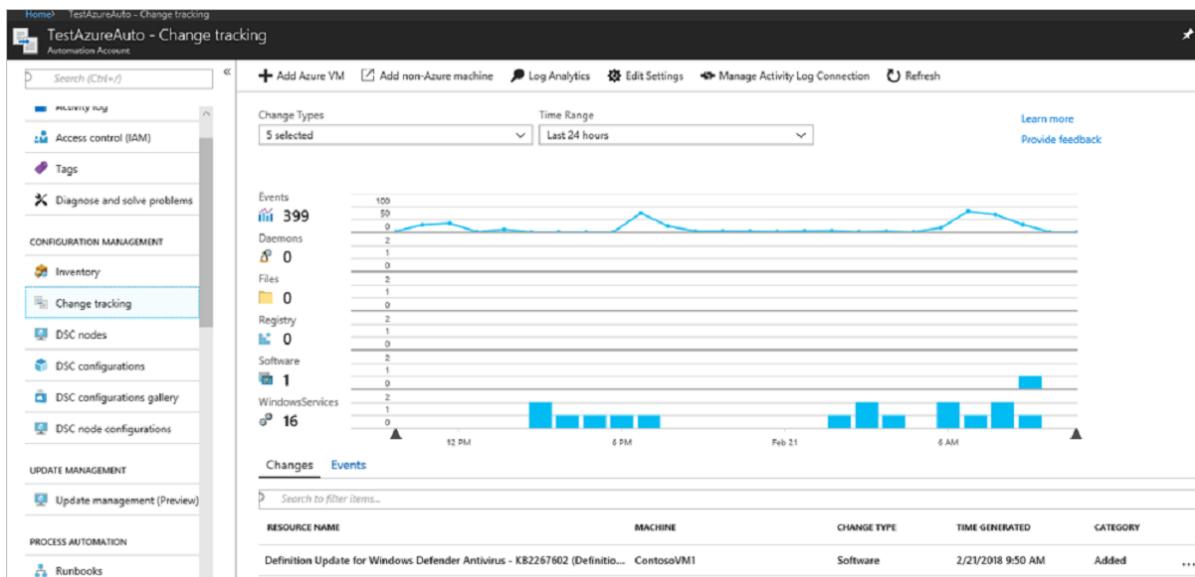


Figure 19: Change management.

#### Learn more:

- Learn about [change tracking](#).
- Learn about [Azure Automation capabilities](#).

## Next steps

Review other best practices:

- [Best practices](#) for networking after migration.
- [Best practices](#) for cost management after migration.

# Azure cloud migration best practices checklist

11/9/2020 • 2 minutes to read • [Edit Online](#)

Start with the [Azure migration guide](#) in the Cloud Adoption Framework if you're interested in migrating to Azure. That guide walks you through a set of tools and basic approaches to migrating virtual machines to the cloud.

The following checklists provide Azure cloud migration best practices that go beyond the basic cloud-native tools. These outline the common areas of complexity that might require the scope of the migration to expand beyond the [Azure migration guide](#).

## Migration best practices for business-driven scope expansion

- **Support global markets:** The business operates in multiple geographic regions with disparate data sovereignty requirements. To meet those requirements, you should factor in additional considerations to the prerequisite review and distribution of assets during migration.

## Migration best practices for technology-driven scope expansion

- **VMware migration:** Migrating VMware hosts can accelerate the overall migration process. Each migrated VMware host can move multiple workloads to the cloud. After migration, those VMs and workloads can stay in VMware, or be migrated to modern cloud capabilities.
- **SQL Server migration:** Migrating instances of SQL Server can accelerate the overall migration process. Each migrated instance can move multiple databases and services, potentially accelerating multiple workloads.
- **Multiple datacenters:** Migrating multiple datacenters adds significant complexity. During each process of the move (assess, migrate, optimize, and manage), additional considerations are discussed to prepare for more complex environments.
- **Data requirements exceed network capacity:** Companies frequently choose to migrate to the cloud because the capacity, speed, or stability of an existing datacenter is no longer satisfactory. Unfortunately, those same constraints add complexity to the migration process, requiring additional planning during the assessment and migration processes.
- **Governance or compliance strategy:** When governance and compliance are vital to the success of a migration, IT governance teams and the cloud adoption team must ensure additional alignment with one another.

## Additional migration best practices

- [Set up networking for workloads migrated to Azure](#)
- [Deploy a migration infrastructure](#)
- [Cost and size workloads migrated to Azure](#)
- [Scale a migration to Azure](#)

## Next steps

The following is a good starting point for reviewing Azure migration best practices.

[Multiple datacenters](#)

# Multiple datacenters

11/9/2020 • 2 minutes to read • [Edit Online](#)

Often the scope of a migration involves the transition of multiple datacenters. The following guidance expands the scope of the [Azure migration guide](#) to address multiple datacenters.

## General scope expansion

Most of the effort required in this scope expansion occurs during the prerequisites, assess, and optimize processes of a migration.

## Suggested prerequisites

Before starting the migration, you should create epics within the project management tool for each datacenter that's to be migrated. Each epic represents a datacenter. It's important to understand the business outcomes and motivations for this migration. Use those motivations to prioritize the list of epics (or datacenters). For instance, if migration is driven by a desire to exit datacenters before leases must be renewed, then each epic would be prioritized based on lease renewal date.

Within each epic, the workloads to be assessed and migrated are managed as features. Each asset within that workload is managed as a user story. The work required to assess, migrate, optimize, promote, secure, and manage each asset is represented as tasks for each asset.

Sprints or iterations then consist of a series of tasks required to migrate the assets and user stories committed to by the cloud adoption team. Releases then consist of one or more workloads or features to be promoted to production.

## Assess process changes

When you're expanding the scope to address multiple datacenters, the biggest change to the assess process is related to the accurate recording and prioritization of workloads and dependencies across datacenters.

### Suggested action during the assess process

**Evaluate cross-datacenter dependencies:** The [dependency visualization tools in Azure Migrate](#) can help pinpoint dependencies. Using this toolset before migration is generally a best practice. But when dealing with global complexity, it becomes a necessary step in the assessment process. Through [dependency grouping](#), the visualization can help identify the IP addresses and ports of any assets required to support the workload.

#### IMPORTANT

- A subject matter expert with an understanding of asset placement and IP address schemas is required to identify assets that reside in a secondary datacenter.
- Evaluate both downstream dependencies and clients in the visualization to understand bidirectional dependencies.

## Migration process changes

Migrating multiple datacenters is similar to consolidating datacenters. After migration, the cloud becomes the singular datacenter solution for multiple assets. The most likely scope expansion during the migration process is the validation and alignment of IP addresses.

## **Suggested action during the migration process**

The following are activities that greatly affect the success of a cloud migration:

- **Evaluate network conflicts:** When you're consolidating datacenters into a single cloud provider, you're likely to create network, DNS, or other conflicts. During migration, it's important to test for conflicts to avoid interruptions to production systems hosted in the cloud.
- **Update routing tables:** Often, modifications to routing tables are required when consolidating networks or datacenters.

## **Optimize and promote process changes**

During optimization, additional testing might be required.

## **Suggested action during the optimize and promote process**

Prior to promotion, provide additional levels of testing during this scope expansion. During testing, it's important to test for routing or other network conflicts. Further, it's important to isolate the deployed application, and retest to validate that all dependencies have been migrated to the cloud. In this case, isolation means separating the deployed environment from production networks. Doing so can catch overlooked assets that are still running on-premises.

## **Secure and manage process changes**

Secure and manage processes are unlikely to be changed by this scope expansion.

## **Next steps**

Return to the checklist to ensure that your migration method is fully aligned.

[Migration best practices checklist](#)

# Azure regions decision guide

11/9/2020 • 15 minutes to read • [Edit Online](#)

Azure comprises many regions around the world. Each [Azure region](#) has specific characteristics that make choosing which region to use incredibly important. These include available services, capacity, constraints, and sovereignty:

- **Available services:** Services that are deployed to each region differ, based on various factors. Select a region for your workload that contains your desired service. For more information, see [Products available by region](#).
- **Capacity:** Each region has a maximum capacity. This can affect which types of subscriptions can deploy which types of services and under what circumstances. This is different than subscription quotas. If you're planning a large-scale datacenter migration to Azure, you might want to consult with your local Azure field team or account manager to confirm that you can deploy at the scale necessary.
- **Constraints:** Certain constraints are placed on the deployment of services in certain regions. For example, some regions are only available as a backup or failover target. Other constraints that are important to note are [data sovereignty requirements](#).
- **Sovereignty:** Certain regions are dedicated to specific sovereign entities. While all regions are Azure regions, these sovereign regions are completely isolated from the rest of Azure. They aren't necessarily managed by Microsoft and might be restricted to certain types of customers. These sovereign regions are:
  - [Azure China](#)
  - [Azure Germany](#): Azure Germany is being deprecated in favor of standard nonsovereign Azure regions in Germany.
  - [Azure US government](#)
  - Two regions in [Australia](#) are managed by Microsoft but are provided for the Australian government and its customers and contractors. Therefore, these regions carry client constraints similar to the other sovereign clouds.

## Operate in multiple geographic regions

When businesses operate in multiple geographic regions, which can be essential for resiliency, this introduces potential complexity in the following forms:

- Asset distribution
- User access profiles
- Compliance requirements
- Regional resiliency

Regional selection is very important to your overall cloud adoption strategy. Let's start with network considerations.

## Network considerations

Any robust cloud deployment requires a well-considered network that takes into account Azure regions. You should account for the following:

- Azure regions are deployed in pairs. In the event of a catastrophic region failure, another region within the same geopolitical boundary is designated as its paired region. Consider deploying into paired regions as a primary and secondary resiliency strategy. One exception to this strategy is [Brazil South](#), which is paired with [South Central US](#). For more information, see [Azure paired regions](#).

- Azure Storage supports [geo-redundant storage \(GRS\)](#). This means that three copies of your data are stored within your primary region, and three additional copies are stored in the paired region. You can't change the storage pairing for GRS.
- Services that rely on Azure Storage GRS can take advantage of this paired region capability. To do so, your applications and the network must be oriented to support that.
- If you don't plan to use GRS to support your regional resiliency needs, you shouldn't use the paired region as your secondary. In the event of a regional failure, there will be intense pressure on resources in the paired region as resources migrate. You can avoid that pressure by recovering to an alternate site and gaining additional speed during your recovery.

**WARNING**

Do not attempt to use Azure GRS for VM backups or recovery. Instead, use [Azure Backup](#) and [Azure Site Recovery](#), along with [Azure managed disks](#), to support your infrastructure as a service (IaaS) workload resiliency.

- Azure Backup and Azure Site Recovery work in tandem with your network design to facilitate regional resiliency for your IaaS and data backup needs. Make sure the network is optimized so data transfers remain on the Microsoft backbone and use [virtual network peering](#), if possible. Some larger organizations with global deployments might instead use [ExpressRoute premium](#), to route traffic between regions and potentially save regional egress charges.
- Azure resource groups are regional specific. It's normal, however, for resources within a resource group to span multiple regions. Consider that in the event of a regional failure, control plane operations against a resource group will fail in the affected region, even though the resources in other regions (within that resource group) will continue to operate. This can affect both your network design and your resource group design.
- Many platform as a service (PaaS) services within Azure support [service endpoints](#) or [Azure Private Link](#). Both of these solutions affect your network considerations substantially with regard to regional resiliency, migration, and governance.
- Many PaaS services rely on their own regional resiliency solutions. For example, both Azure SQL Database and Azure Cosmos DB allow you to easily replicate to additional regions. Services such as Azure DNS don't have regional dependencies. As you consider which services you will use in your adoption process, make sure to clearly understand the failover capabilities and recovery steps that can be required for each Azure service.
- In addition to deploying to multiple regions to support disaster recovery, many organizations choose to deploy in an active-active pattern to not rely on failover. This method offers the additional benefits of global load balancing, additional fault tolerance, and network performance boosts. To take advantage of this pattern, your applications must support running active-active in multiple regions.

**WARNING**

Azure regions are highly available constructs, with SLAs applied to the services running in them. But you should never take a single region dependency on mission-critical applications. Always plan for regional failure, and practice recovery and mitigation steps.

After considering the network topology, you must next look at additional documentation and process alignment that might be necessary. The following approach can help assess the potential challenges and establish a general course of action:

- Consider a more robust readiness and governance implementation.
- Inventory the affected geographies. Compile a list of the regions and countries that are affected.

- Document data sovereignty requirements. Do the countries identified have compliance requirements that govern data sovereignty?
- Document the user base. Will employees, partners, or customers in the identified country be affected by the cloud migration?
- Document datacenters and assets. Are there assets in the identified country that might be included in the migration effort?
- Document regional SKU availability and failover requirements.

Align changes across the migration process to address the initial inventory.

## Document complexity

The following table can aid in documenting the findings from the previous steps:

REGION	COUNTRY	LOCAL EMPLOYEES	LOCAL EXTERNAL USERS	LOCAL DATACENTERS OR ASSETS	DATA SOVEREIGNTY REQUIREMENTS
North America	United States	Yes	Partners and customers	Yes	No
North America	Canada	No	Customers	Yes	Yes
Europe	Germany	Yes	Partners and customers	No - network only	Yes
Asia Pacific	South Korea	Yes	Partners	Yes	No

## Relevance of data sovereignty

Around the world, government organizations have begun establishing data sovereignty requirements, like General Data Protection Regulation (GDPR). Compliance requirements of this nature often require localization within a specific region or even within a specific country to protect their citizens. In some cases, data pertaining to customers, employees, or partners must be stored on a cloud platform within the same region as the end user.

Addressing this challenge has been a significant motivation for cloud migrations for companies that operate on a global scale. To maintain compliance requirements, some companies have chosen to deploy duplicate IT assets to cloud providers within the region. In the preceding table, Germany is a good example of this scenario. This example includes customers, partners, and employees but not current IT assets in Germany. This company might choose to deploy some assets to a datacenter within the GDPR area, potentially using the German Azure datacenters. An understanding of the data affected by GDPR would help the cloud adoption team understand the best migration approach in this case.

### Why is the location of end users relevant?

Companies that support end users in multiple countries have developed technical solutions for addressing end-user traffic. In some cases, this involves localization of assets. In other scenarios, the company might choose to implement global wide area network (WAN) solutions to address disparate user bases via network focused solutions. In either case, the migration strategy can be affected by the usage profiles of those disparate end users.

Because the company supports employees, partners, and customers in Germany without currently having datacenters there, this company probably implemented a leased-line solution. This type of solution routes traffic to datacenters in other countries. This existing routing presents a significant risk to the perceived performance of migrated applications. Injecting additional hops in an established and tuned global WAN can create the perception of underperforming applications after migration. Finding and fixing those issues can add significant delays to a

project.

In each of the following processes, guidance for addressing this complexity is included across prerequisites, assess, migrate, and optimize processes. Understanding user profiles in each country is critical to properly manage this complexity.

### Why is the location of datacenters relevant?

The location of existing datacenters can affect a migration strategy. For example:

**Architecture decisions:** The target region is one of the first steps in migration strategy design. This is often influenced by the location of the existing assets. Additionally, the availability of cloud services and the unit cost of those services can vary from one region to the next. Understanding where current and future assets are located affects architecture decisions and can influence budget estimates.

**Datacenter dependencies:** The data in the preceding table shows that dependencies between various global datacenters are likely. Those dependencies might not be documented or understood clearly in many organizations that operate on this type of scale. Your company's approach to evaluating user profiles helps to identify some of these dependencies in your organization. In addition, your team should explore additional assessment steps that can mitigate the risks and complexities that arise from dependencies.

## Implement the general approach

The following approach uses a data-driven model for addressing global migration complexities. When the scope for a migration includes multiple regions, the cloud adoption team should evaluate the following readiness considerations:

- Data sovereignty might require localization of some assets, but many assets might not be governed by those compliance constraints. Things like logging, reporting, network routing, identity, and other central IT services might be eligible to be hosted as shared services across multiple subscriptions, or even multiple regions. The cloud adoption team should evaluate by using a shared service model for those services, as outlined in the [reference architecture for a hub and spoke topology with shared services](#).
- When you're deploying multiple instances of similar environments, an environment factory can create consistency, improve governance, and accelerate deployment. The [governance guide for complex enterprises](#) establishes an approach that creates an environment that scales across multiple regions.

When the team is comfortable with the baseline approach and readiness is aligned, you should then consider a few data-driven prerequisites:

- **General discovery:** Complete the [documenting complexity](#) table.
- **Perform a user profile analysis on each affected country:** It's important to understand general end-user routing early in the migration process. Changing global lease lines and adding connections like ExpressRoute to a cloud datacenter can require months of networking delays. Address this as early in the process as possible.
- **Initial digital estate rationalization:** Whenever complexity is introduced into a migration strategy, you should complete an initial digital estate rationalization. See the guidance on [digital estate rationalization](#).
  - **Additional digital estate requirements:** Establish tagging policies to identify any workload affected by data sovereignty requirements. Required tags should begin in the digital estate rationalization and carry through to the migrated assets.
- **Evaluate a hub-and-spoke model:** Distributed systems often share common dependencies. Those dependencies can often be addressed through the implementation of a hub-and-spoke model. While such a model is out of scope for the migration process, it should be flagged for consideration during future iterations of the [ready processes](#).
- **Prioritization of the migration backlog:** When network changes are required to support the production deployment of a workload that supports multiple regions, the cloud strategy team should track and manage escalations regarding those network changes. The higher level of executive support helps to accelerate the

change by freeing the strategy team to reprioritize the backlog and ensure that global workloads aren't blocked by network changes. Such workloads should only be prioritized after the network changes are complete.

These prerequisites help establish processes that can address this complexity during execution of the migration strategy.

## Assess process changes

When facing global asset and user base complexities in migration scenarios, you should add a few key activities to assessing your migration candidates. These activities produce data to clarify obstacles and outcomes for global users and assets.

### Suggested action during the assess process

**Evaluate cross-datacenter dependencies:** The [dependency visualization tools in Azure Migrate](#) can help pinpoint dependencies. Using these tools before migration is a best practice. When dealing with global complexity, it becomes a necessary step to the assessment process. Through [dependency grouping](#), the visualization can help identify the IP addresses and ports of any assets required to support the workload.

#### IMPORTANT

- A subject matter expert with an understanding of asset placement and IP address schemas is required to identify assets that reside in a secondary datacenter.
- Evaluate both downstream dependencies and clients in the visualization to understand bidirectional dependencies.

**Identify global user impact:** The outputs from the prerequisite user profile analysis should identify any workload affected by global user profiles. When a migration candidate is in the affected workload list, the architect preparing for migration should consult networking and operations subject matter experts. They help to validate network routing and performance expectations. At a minimum, the architecture should include an ExpressRoute connection between the closest network operations center and Azure. The [reference architecture for ExpressRoute](#) connections can aid in the configuration of the necessary connection.

**Design for compliance:** The outputs from the prerequisite user profile analysis should identify any workload affected by data sovereignty requirements. During the architecture activities of the assess process, the assigned architect should consult compliance subject matter experts. They help to understand any requirements for migration and deployment across multiple regions. Those requirements significantly affect design strategies. The reference architectures for [multiregion web applications](#) and [multiregion n-tier applications](#) can assist design.

#### WARNING

When you're using either of the reference architectures above, it might be necessary to exclude specific data elements from replication processes to adhere to data sovereignty requirements. This will add an additional step to the promotion process.

## Migration process changes

When you're migrating an application that must be deployed to multiple regions, the cloud adoption team must account for a few considerations. These consist of Azure Site Recovery vault design, configuration and process server design, network bandwidth designs, and data synchronization.

### Suggested action during the migration process

**Azure Site Recovery vault design:** Azure Site Recovery is the suggested tool for cloud-native replication and synchronization of digital assets to Azure. Site Recovery replicates data about the asset to a Site Recovery vault, which is bound to a specific subscription in a specific region and Azure datacenter. When you're replicating assets to a second region, you might also need a second Site Recovery vault.

**Configuration and process server design:** Site Recovery works with a local instance of a configuration and process server, which is bound to a single Site Recovery vault. This means that you might need to install a second instance of these servers in the source datacenter to facilitate replication.

**Network bandwidth design:** During replication and ongoing synchronization, you move binary data over the network, from the source datacenter to the Site Recovery vault in the target Azure datacenter. This process consumes bandwidth. Duplication of the workload to a second region doubles the amount of bandwidth consumed. When bandwidth is limited or a workload involves a large amount of configuration or data drift, it can interfere with the time required to complete the migration. More importantly, it can affect the experience of users or applications that still depend on the bandwidth of the source datacenter.

**Data synchronization:** Often the largest bandwidth drain comes from synchronization of the data platform. As defined in the reference architectures for [multiregion web applications](#) and [multiregion n-tier applications](#), data synchronization is often required to keep the applications aligned. If this is the desired operational state of the application, it might be wise to complete a synchronization between the source data platform and each of the cloud platforms. You should do this before migrating the application and middle tier assets.

**Azure-to-Azure disaster recovery:** An alternative option can reduce complexity further. If timelines and data synchronization approach a two-step deployment, [Azure-to-Azure disaster recovery](#) might be an acceptable solution. In this scenario, you migrate the workload to the first Azure datacenter by using a single Site Recovery vault and configuration or process server design. After you test the workload, you can recover it to a second Azure datacenter from the migrated assets. This approach reduces the impact to resources in the source datacenter and takes advantage of faster transfer speeds and high bandwidth limits available between Azure datacenters.

**NOTE**

This approach can increase short-term migration costs through additional egress bandwidth charges.

## Optimize and promote process changes

As you address global complexity during optimization and promotion, you might require duplicated efforts in each of the additional regions. When a single deployment is acceptable, you might still need to duplicate business testing and business change plans.

### Suggested action during the optimize and promote process

**Pretest optimization:** Initial automation testing can identify potential optimization opportunities, as with any migration effort. In the case of global workloads, test the workload in each region independently. Minor configuration changes in the network or the target Azure datacenter can affect performance.

**Business change plans:** For any complex migration scenario, create a business change plan. This ensures clear communication regarding any changes to business processes, user experiences, and the timing of efforts required to integrate the changes. In the case of global migration efforts, the plan should include considerations for end users in each affected geography.

**Business testing:** In conjunction with the business change plan, business testing might be required in each region. This ensures adequate performance and adherence to the modified networking routing patterns.

**Promotion flights:** Often promotion happens as a single activity, rerouting production traffic to the migrated workloads. In the case of global release efforts, you should deliver promotion in flights (or predefined collections of users). This allows the cloud strategy team and the cloud adoption team to better observe performance and improve support of users in each region. Promotion flights are often controlled at the networking level by changing the routing of specific IP ranges from the source workload assets to the newly migrated assets. After a specified collection of end users have been migrated, the next group can be rerouted.

**Flight optimization:** One of the benefits of promotion flights is that it allows for deeper observations and

additional optimization of the deployed assets. After a brief period of production usage by the first flight, additional refinement of the migrated assets is suggested, when allowed by IT operation procedures.

# Best practices when data requirements exceed network capacity during a migration effort

11/9/2020 • 5 minutes to read • [Edit Online](#)

In a cloud migration, you replicate and synchronize assets over the network between the existing datacenter and the cloud. It's not uncommon for the existing data size requirements of various workloads to exceed network capacity. In such a scenario, the process of migration can be radically slowed, or in some cases, stopped entirely. The following guidance expands the scope of the [Azure migration guide](#) to provide a solution that works around network limitations.

## General scope expansion

Most of the effort required in this scope expansion occurs during the prerequisites, assess, and migrate phases of a migration.

## Suggested prerequisites

**Validate network capacity risks:** [Digital estate rationalization](#) is a highly recommended prerequisite, especially if there are concerns of overburdening the available network capacity. During digital estate rationalization, you collect an [inventory of digital assets](#). That inventory should include existing storage requirements across the digital estate.

As outlined in [Replication risks: physics of replication](#), you can use that inventory to estimate total migration data size, which can be compared to total available migration bandwidth. If that comparison doesn't align with the required time to business change, then this article can help accelerate migration velocity reducing the time required to migrate the datacenter.

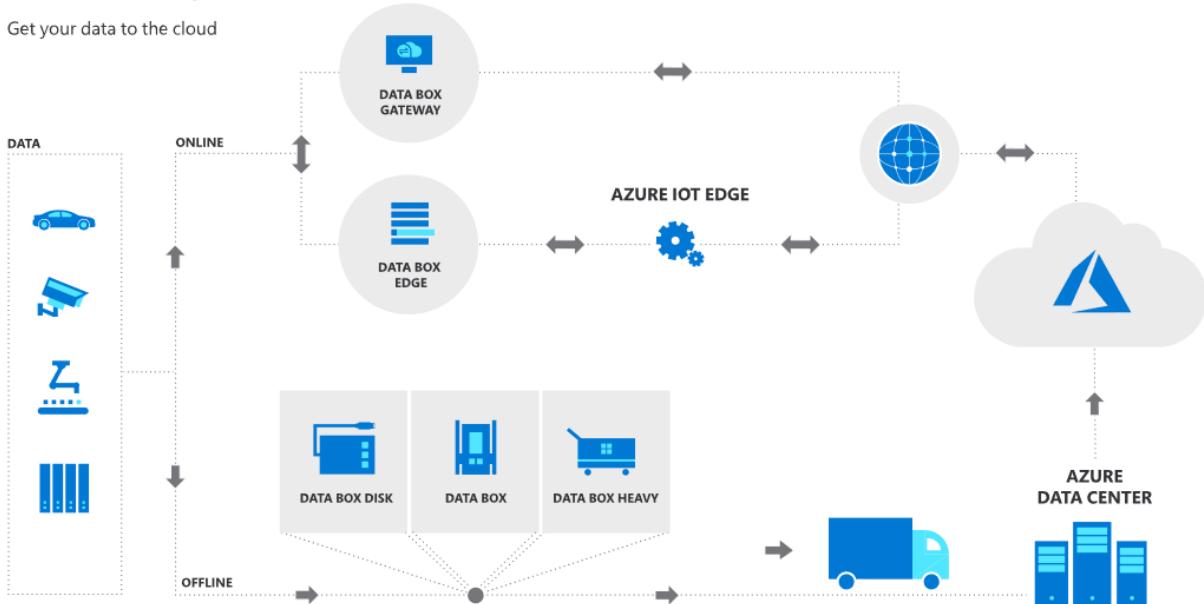
**Offline transfer of independent data stores:** The following diagram shows examples of both online and offline data transfers with Azure Data Box. You can use these approaches to ship large volumes of data to the cloud, prior to workload migration. In an offline data transfer, you copy source data to Azure Data Box, which is then physically shipped to Microsoft for transfer into an Azure Storage account as a file or a blob. Prior to other migration efforts, you can use this process to ship data that isn't directly tied to a specific workload. Doing this reduces the amount of data that needs to be shipped over the network and supports completing a migration within network constraints.

You can use this approach to transfer data from HDFS, backups, archives, file servers, and applications. Existing technical guidance explains how to use this approach to transfer data from an [HDFS store](#) or from disks by using [SMB](#), [NFS](#), [rest](#), or [data copy service](#) to Data Box.

There are also third-party partner solutions that use Azure Data Box for a migration. With these solutions, you move a large volume of data via an offline transfer, but you synchronize it later at a lower scale over the network.

# DATA BOX

Get your data to the cloud



## Assess process changes

If the storage requirements of a workload (or workloads) exceed network capacity, then you can still use Azure Data Box in an offline data transfer.

Network transmission is the recommended approach unless the network is unavailable. The speed of transferring data over the network, even when bandwidth is constrained, is typically faster than physically shipping the data by using an offline transfer mechanism.

If connectivity to Azure is available, you should conduct an analysis before using Data Box, especially if migration of the workload is time sensitive. Data Box is only advisable when the time to transfer the necessary data exceeds the time to populate, ship, and restore it.

### Suggested action during the assess process

**Network capacity analysis:** When workload-related data transfer requirements are at risk of exceeding network capacity, the cloud adoption team adds an additional analysis task to the assess process called network capacity analysis. During this analysis, a member of the team estimates the amount of available network capacity and required data transfer time. Note that this team member should have subject matter expertise regarding the local network and network connectivity.

Available capacity is compared to the storage requirements of all assets to be migrated during the current release. If the storage requirements exceed the available bandwidth, then assets supporting the workload are selected for offline transfer.

#### IMPORTANT

At the conclusion of the analysis, you might need to update the release plan to reflect the time required to ship, restore, and synchronize the assets to be transferred offline.

**Drift analysis:** Analyze each asset to be transferred offline for storage and configuration drift. *Storage drift* is the amount of change in the underlying storage over time. *Configuration drift* is change in the configuration of the asset over time. From the time the storage is copied to the time the asset is promoted to production, any drift might be lost. If that drift needs to be reflected in the migrated asset, you'll need to synchronize the local asset and the migrated asset. Flag this for consideration during migration execution.

# Migration process changes

When you're using offline transfer mechanisms, [replication processes](#) aren't typically required, whereas [synchronization processes](#) might still be necessary. If an asset is being transferred offline, understanding the drift analysis results from the assess process will inform the tasks required during migration.

## Suggested action during the migration process

**Copy storage:** You can use this approach to transfer data of HDFS, backups, archives, file servers, or applications. Existing technical guidance explains how to use this approach to transfer data from an [HDFS store](#) or from disks by using [SMB, NFS, rest](#), or [data copy service](#) to Data Box.

There are also third-party partner solutions that use Azure Data Box for a migration. With these solutions, you move a large volume of data via an offline transfer, but you synchronize it later at a lower scale over the network.

**Ship the device:** After you copy the data, you can [ship the device to Microsoft](#). After the data is received and imported, it's available in an Azure Storage account.

**Restore the asset:** [Verify that the data](#) is available in the storage account. If so, you can use the data as a blob or in Azure Files. If the data is a VHD/VHDX file, you can convert the file to managed disks. Those managed disks can then be used to instantiate a virtual machine, which creates a replica of the original on-premises asset.

**Synchronization:** If synchronization of drift is a requirement for a migrated asset, you can use one of the third-party partner solutions to synchronize the files until the asset is restored.

## Optimize and promote process changes

Optimize activities aren't likely to be affected by this change in scope.

## Secure and manage process changes

Secure and manage activities aren't likely to be affected by this change in scope.

## Next steps

Return to the checklist to ensure that your migration method is fully aligned.

[Migration best practices checklist](#)

# Best practices to set up networking for workloads migrated to Azure

11/9/2020 • 28 minutes to read • [Edit Online](#)

As you plan and design for migration, in addition to the migration itself, one of the most critical steps is the design and implementation of Azure networking. This article describes best practices for networking when you're migrating to infrastructure as a service (IaaS) and platform as a service (PaaS) implementations in Azure.

## IMPORTANT

The best practices and opinions described in this article are based on the Azure platform and service features available at the time of writing. Features and capabilities change over time. Not all recommendations might be applicable for your deployment, so select those that work for you.

## Design virtual networks

Azure provides virtual networks with these capabilities:

- Azure resources communicate privately, directly, and securely with each other over virtual networks.
- You can configure endpoint connections on virtual networks for VMs and services that require internet communication.
- A virtual network is a logical isolation of the Azure cloud that's dedicated to your subscription.
- You can implement multiple virtual networks within each Azure subscription and Azure region.
- Each virtual network is isolated from other virtual networks.
- Virtual networks can contain private and public IP addresses defined in [RFC 1918](#), expressed in CIDR notation. Public IP addresses specified in a virtual network's address space aren't directly accessible from the internet.
- Virtual networks can connect to each other by using virtual network peering. Connected virtual networks can be in the same or different regions. Thus, resources in one virtual network can connect to resources in other virtual networks.
- By default, Azure routes traffic between subnets within a virtual network, connected virtual networks, on-premises networks, and the internet.

When planning your virtual network topology, you should consider how to arrange IP address spaces, how to implement a hub-and-spoke network, how to segment virtual networks into subnets, setting up DNS, and implementing Azure Availability Zones.

## Best practice: Plan IP addressing

When you create virtual networks as part of your migration, it's important to plan out your virtual network IP address space.

You should assign an address space that isn't larger than a CIDR range of /16 for each virtual network. Virtual networks allow for the use of 65,536 IP addresses. Assigning a smaller prefix than /16, such as a /15, which has 131,072 addresses, will result in the excess IP addresses becoming unusable elsewhere. It's important not to waste IP addresses, even if they're in the private ranges defined by RFC 1918.

Other tips for planning are:

- The virtual network address space shouldn't overlap with on-premises network ranges.

- Don't use network address translation (NAT).
- Overlapping addresses can cause networks that can't be connected, and routing that doesn't work properly. If networks overlap, you'll need to redesign the network or use NAT.

#### Learn more:

- Read the [Azure Virtual Network overview](#).
- Review the [Azure Virtual Network FAQ](#).
- Learn about [Azure networking limits](#).

## Best practice: Implement a hub-and-spoke network topology

A hub-and-spoke network topology isolates workloads while sharing services, such as identity and security. The hub is an Azure virtual network that acts as a central point of connectivity. The spokes are virtual networks that connect to the hub virtual network by using peering. Shared services are deployed in the hub, while individual workloads are deployed as spokes.

Consider the following:

- Implementing a hub-and-spoke topology in Azure centralizes common services, such as connections to on-premises networks, firewalls, and isolation between virtual networks. The hub virtual network provides a central point of connectivity to on-premises networks, and a place to host services used by workloads hosted in spoke virtual networks.
- A hub-and-spoke configuration is typically used by larger enterprises. Smaller networks might consider a simpler design to save on costs and complexity.
- You can use spoke virtual networks to isolate workloads, with each spoke managed separately from other spokes. Each workload can include multiple tiers, and multiple subnets that are connected with Azure load balancers.
- You can implement hub-and-spoke virtual networks in different resource groups, and even in different subscriptions. When you peer virtual networks in different subscriptions, the subscriptions can be associated to the same, or different, Azure Active Directory (Azure AD) tenants. This allows for decentralized management of each workload, while sharing services maintained in the hub network.

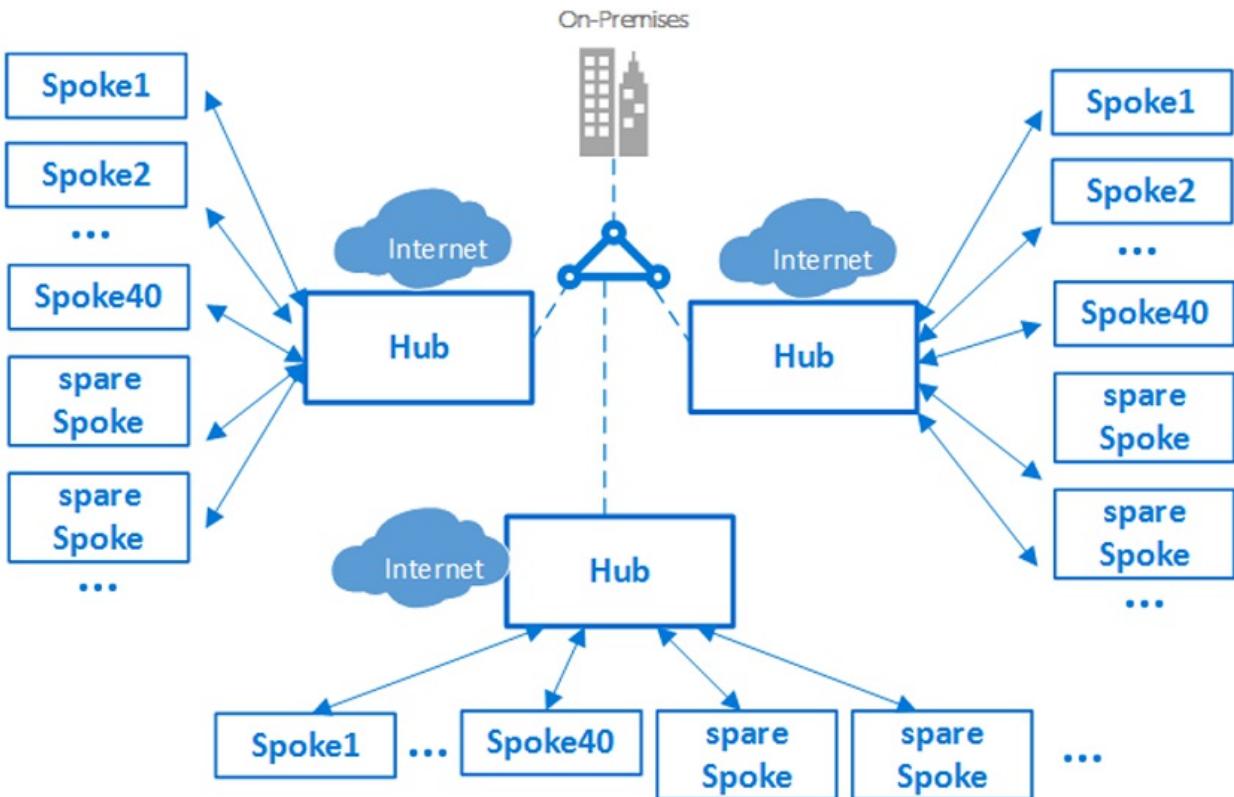


Figure 1: Hub-and-spoke topology.

#### Learn more:

- Read about a [hub-and-spoke topology](#).
- Get network recommendations for running [Windows VMs](#) and [Linux VMs](#) in Azure.
- Learn about [virtual network peering](#).

## Best practice: Design subnets

To provide isolation within a virtual network, you segment it into one or more subnets, and allocate a portion of the virtual network's address space to each subnet.

- You can create multiple subnets within each virtual network.
- By default, Azure routes network traffic between all subnets in a virtual network.
- Your subnet decisions are based on your technical and organizational requirements.
- You create subnets by using CIDR notation.

When you're deciding on network range for subnets, be aware that Azure retains five IP addresses from each subnet that can't be used. For example, if you create the smallest available subnet of `/29` (with eight IP addresses), Azure will retain five addresses. In this case, you only have three usable addresses that can be assigned to hosts on the subnet. For most cases, use `/28` as the smallest subnet.

#### Example:

The table shows an example of a virtual network with an address space of `10.245.16.0/20` segmented into subnets, for a planned migration.

SUBNET	CIDR	ADDRESSES	USAGE
DEV-FE-EUS2	10.245.16.0/22	1019	Front-end or web-tier VMs

SUBNET	CIDR	ADDRESSES	USAGE
DEV-APP-EUS2	10.245.20.0/22	1019	App-tier VMs
DEV-DB-EUS2	10.245.24.0/23	507	Database VMs

**Learn more:**

- Learn about [designing subnets](#).
- Learn how Contoso, a fictional company, [prepared their networking infrastructure for migration](#).

## Best practice: Set up a DNS server

Azure adds a DNS server by default when you deploy a virtual network. This allows you to rapidly build virtual networks and deploy resources. But this DNS server only provides services to the resources on that virtual network. If you want to connect multiple virtual networks together, or connect to an on-premises server from virtual networks, you need additional name resolution capabilities. For example, you might need Active Directory to resolve DNS names between virtual networks. To do this, you deploy your own custom DNS server in Azure.

- DNS servers in a virtual network can forward DNS queries to the recursive resolvers in Azure. This enables you to resolve host names within that virtual network. For example, a domain controller that runs in Azure can respond to DNS queries for its own domains, and forward all other queries to Azure.
- DNS forwarding allows VMs to see both your on-premises resources (via the domain controller) and Azure-provided host names (using the forwarder). You can access the recursive resolvers in Azure by using the virtual IP address `168.63.129.16`.
- DNS forwarding also enables DNS resolution between virtual networks, and allows on-premises machines to resolve host names provided by Azure.
  - To resolve a VM host name, the DNS server VM must reside in the same virtual network, and be configured to forward host name queries to Azure.
  - Because the DNS suffix is different in each virtual network, you can use conditional forwarding rules to send DNS queries to the correct virtual network for resolution.
- When you use your own DNS servers, you can specify multiple DNS servers for each virtual network. You can also specify multiple DNS servers per network interface (for Azure Resource Manager), or per cloud service (for the classic deployment model).
- DNS servers specified for a network interface or cloud service take precedence over DNS servers specified for the virtual network.
- In Azure Resource Manager, you can specify DNS servers for a virtual network and a network interface, but the best practice is to use the setting only on virtual networks.

The screenshot shows the Azure portal interface for managing DNS servers in a virtual network. The top navigation bar displays the virtual network name: "VNET-HUB-EUS2 - DNS servers". On the left, a sidebar menu includes "Overview", "Activity log", "Access control (IAM)", "Tags", and "Diagnose and solve problems". The main content area is titled "DNS servers" and shows two options: "Default (Azure-provided)" and "Custom". The "Custom" option is selected, and a list of three IP addresses is displayed: 172.16.0.10, 172.16.0.11, and 168.63.129.16. Each entry has a "..." button to its right. At the bottom, there is a button labeled "Add DNS server" with its own "..." button.

Figure 2: DNS servers for a virtual network.

#### Learn more:

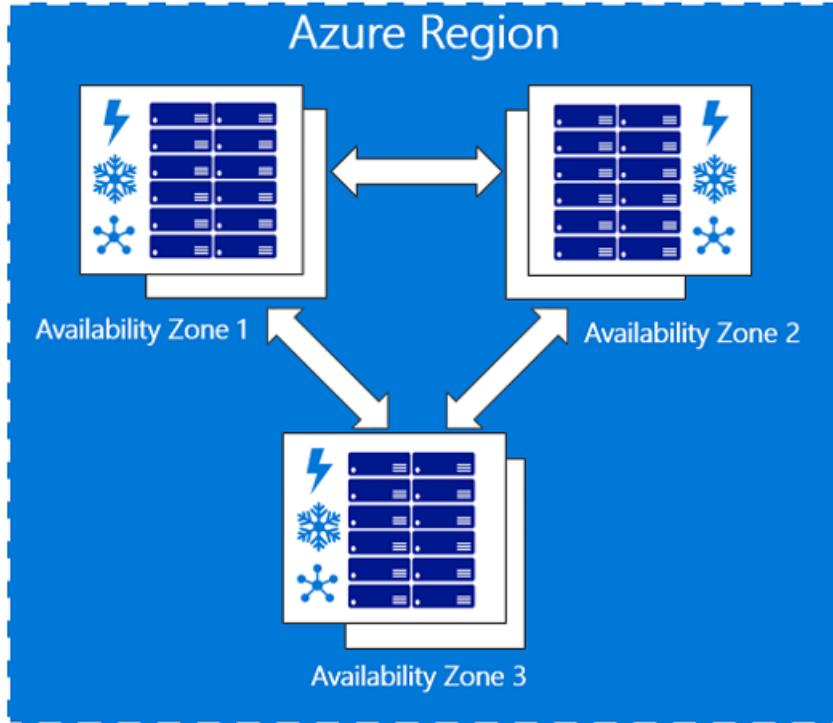
- Learn about [name resolution when you use your own DNS server](#).
- Learn about [DNS naming rules and restrictions](#).

## Best practice: Set up Availability Zones

Availability Zones increase high-availability to protect your applications and data from datacenter failures. Availability Zones are unique physical locations within an Azure region. Each zone is made up of one or more datacenters equipped with independent power, cooling, and networking. To ensure resiliency, there's a minimum of three separate zones in all enabled regions. The physical separation of Availability Zones within a region protects applications and data from datacenter failures.

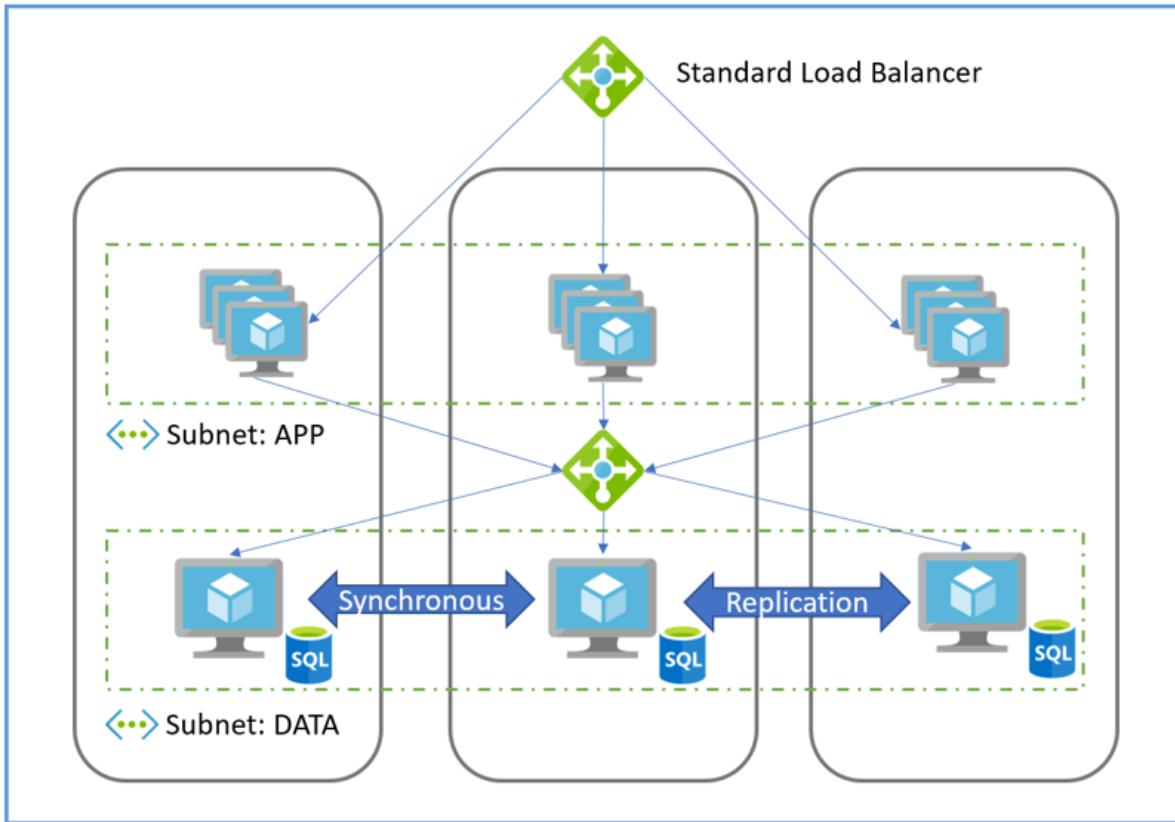
Here are a few additional points to be aware of as you set up Availability Zones:

- Zone-redundant services replicate your applications and data across Availability Zones to protect from single points of failure.
- With Availability Zones, Azure offers an SLA of 99.99 percent VM uptime.



*Figure 3: Availability Zones.*

- You can plan and build high-availability into your migration architecture by colocating compute, storage, networking, and data resources within a zone, and replicating them in other zones. Azure services that support Availability Zones fall into two categories:
  - **Zonal services:** You associate a resource with a specific zone, such as VMs, managed disks, or IP addresses.
  - **Zone-redundant services:** The resource replicates automatically across zones, such as zone-redundant storage or Azure SQL Database.
- To provide zonal fault tolerance, you can deploy a standard Azure load balancer with internet-facing workloads or application tiers.



Azure Region

Figure 4: Load balancer.

#### Learn more:

- Read the [Availability Zones overview](#).

## Design hybrid cloud networking

For a successful migration, it's critical to connect on-premises corporate networks to Azure. This creates an always-on connection known as a hybrid-cloud network, where services are provided from the Azure cloud to corporate users. There are two options for creating this type of network:

- **Site-to-site VPN:** You establish a site-to-site connection between your compatible on-premises VPN device and an Azure VPN gateway that's deployed in a virtual network. Any authorized, on-premises resource can access virtual networks. Site-to-site communications are sent through an encrypted tunnel over the internet.
- **Azure ExpressRoute:** You establish an Azure ExpressRoute connection between your on-premises network and Azure, through an ExpressRoute partner. This connection is private, and traffic doesn't go over the internet.

#### Learn more:

- Learn more about [hybrid-cloud networking](#).

## Best practice: Implement a highly available site-to-site VPN

To implement a site-to-site VPN, you set up a VPN gateway in Azure.

- A VPN gateway is a specific type of virtual network gateway. It sends encrypted traffic between an Azure virtual network and an on-premises location over the public internet.
- A VPN gateway can also send encrypted traffic between Azure virtual networks over the Microsoft network.
- Each virtual network can have only one VPN gateway.
- You can create multiple connections to the same VPN gateway. When you create multiple connections, all VPN tunnels share the available gateway bandwidth.

Every Azure VPN gateway consists of two instances in an active-standby configuration:

- For planned maintenance or unplanned disruption to the active instance, failover occurs and the standby instance takes over automatically. This instance resumes the site-to-site or network-to-network connection.
- The switchover causes a brief interruption.
- For planned maintenance, connectivity should be restored within 10 to 15 seconds.
- For unplanned issues, the connection recovery takes longer, up to 1.5 minutes in the worst case.
- Point-to-site VPN client connections to the gateway are disconnected, and users need to reconnect from client machines.

When setting up a site-to-site VPN:

- You need a virtual network whose address range doesn't overlap with the on-premises network to which the VPN will connect.
- You create a gateway subnet in the network.
- You create a VPN gateway, specify the gateway type (VPN), and whether the gateway is policy-based or route-based. A route-based VPN is considered more capable and future-proof.
- You create a local network gateway on-premises, and configure your on-premises VPN device.
- You create a failover site-to-site VPN connection between the virtual network gateway and the on-premises device. Using route-based VPN allows for either active-passive or active-active connections to Azure. The route-based option also supports both site-to-site (from any computer) and point-to-site (from a single computer) connections, concurrently.
- You specify the gateway SKU that you want to use. This depends on your workload requirements, throughput, features, and SLAs.
- Border gateway protocol (BGP) is an optional feature. You can use it with Azure ExpressRoute and route-based VPN gateways to propagate your on-premises BGP routes to your virtual networks.

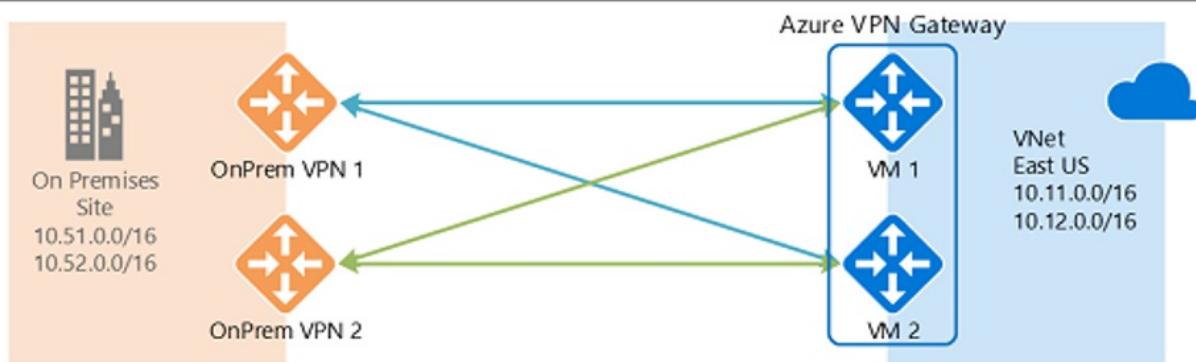


Figure 5: Site-to-site VPN.

#### Learn more:

- Review [compatible on-premises VPN devices](#).
- Read the [Azure VPN gateways overview](#).
- Learn about [highly available VPN connections](#).
- Learn about [planning and designing a VPN gateway](#).
- Review [VPN gateway settings](#).
- Review [gateway SKUs](#).
- Read about [setting up BGP with Azure VPN gateways](#).

#### Best practice: Configure a gateway for VPN gateways

When you create a VPN gateway in Azure, you must use a special subnet named `GatewaySubnet`. When you create this subnet, note these best practices:

- **GatewaySubnet** can have a maximum prefix length of 29 (for example, `10.119.255.248/29`). The current recommendation is that you use a prefix length of 27 (for example, `10.119.255.224/27`).
- When you define the address space of the gateway subnet, use the very last part of the virtual network address space.
- When you're using the Azure gateway subnet, never deploy any VMs or other devices, such as Azure Application Gateway, to the gateway subnet.
- Don't assign a network security group (NSG) to this subnet. It will cause the gateway to stop functioning.

**Learn more:**

- [Use this tool](#) to determine your IP address space.

## Best practice: Implement Azure Virtual WAN for branch offices

For multiple VPN connections, Azure Virtual WAN is a networking service that provides optimized and automated, branch-to-branch connectivity through Azure.

- Virtual WAN allows you to connect and configure branch devices to communicate with Azure. You can do this manually, or by using preferred provider devices through an Azure Virtual WAN partner.
- Using preferred provider devices allows for simple use, connectivity, and configuration management.
- The Azure Virtual WAN built-in dashboard provides instant troubleshooting insights that save time, and provide an easy way to track large-scale, site-to-site connectivity.

**Learn more:** Learn about [Azure Virtual WAN](#).

## Best practice: Implement ExpressRoute for mission-critical connections

The Azure ExpressRoute service extends your on-premises infrastructure into the Microsoft cloud, by creating private connections between the virtual Azure datacenter and on-premises networks. Here are a few implementation details:

- ExpressRoute connections can be over an any-to-any (IP VPN) network, a point-to-point Ethernet network, or through a connectivity provider. They don't go over the public internet.
- ExpressRoute connections offer higher security, reliability, and higher speeds (up to 10 Gbps), along with consistent latency.
- ExpressRoute is useful for virtual datacenters, as customers can get the benefits of compliance rules associated with private connections.
- With ExpressRoute Direct, you can connect directly to Microsoft routers at 100 Gbps, for larger bandwidth needs.
- ExpressRoute uses BGP to exchange routes between on-premises networks, Azure instances, and Microsoft public addresses.

Deploying ExpressRoute connections usually involves engaging with an ExpressRoute service provider. For a rapid start, it's common to initially use a site-to-site VPN to establish connectivity between the virtual datacenter and on-premises resources. Then you migrate to an ExpressRoute connection when a physical interconnection with your service provider is established.

**Learn more:**

- Read an [overview](#) of ExpressRoute.
- Learn about [ExpressRoute Direct](#).

## Best practice: Optimize ExpressRoute routing with BGP communities

When you have multiple ExpressRoute circuits, you have more than one path to connect to Microsoft. As a result, suboptimal routing can happen and your traffic might take a longer path to reach Microsoft, and Microsoft to your network. The longer the network path, the higher the latency. Latency directly affects application performance and

the user experience.

### Example:

Let's review an example:

- You have two offices in the US, one in Los Angeles and one in New York City.
- Your offices are connected on a WAN, which can be either your own backbone network or your service provider's IP VPN.
- You have two ExpressRoute circuits, one in `West US` and one in `East US`, that are also connected on the WAN. Obviously, you have two paths to connect to the Microsoft network.

### Problem:

Now imagine that you have an Azure deployment (for example, Azure App Service) in both `West US` and `East US`.

- You want users in each office to access their nearest Azure services for an optimal experience.
- Thus, you want to connect users in Los Angeles to Azure `West US`, and users in New York to Azure `East US`.
- This works for east coast users, but not for those on the west coast. The problem is:
  - On each ExpressRoute circuit, we advertise both prefixes in Azure: `East US` (`23.100.0.0/16`) and Azure `West US` (`13.100.0.0/16`).
  - Without knowing which prefix is from which region, prefixes aren't treated differently.
  - Your WAN network can assume that both prefixes are closer to `East US` than `West US`, and thus route users from both offices to the ExpressRoute circuit in `East US`. This provides a worse experience for users in the Los Angeles office.

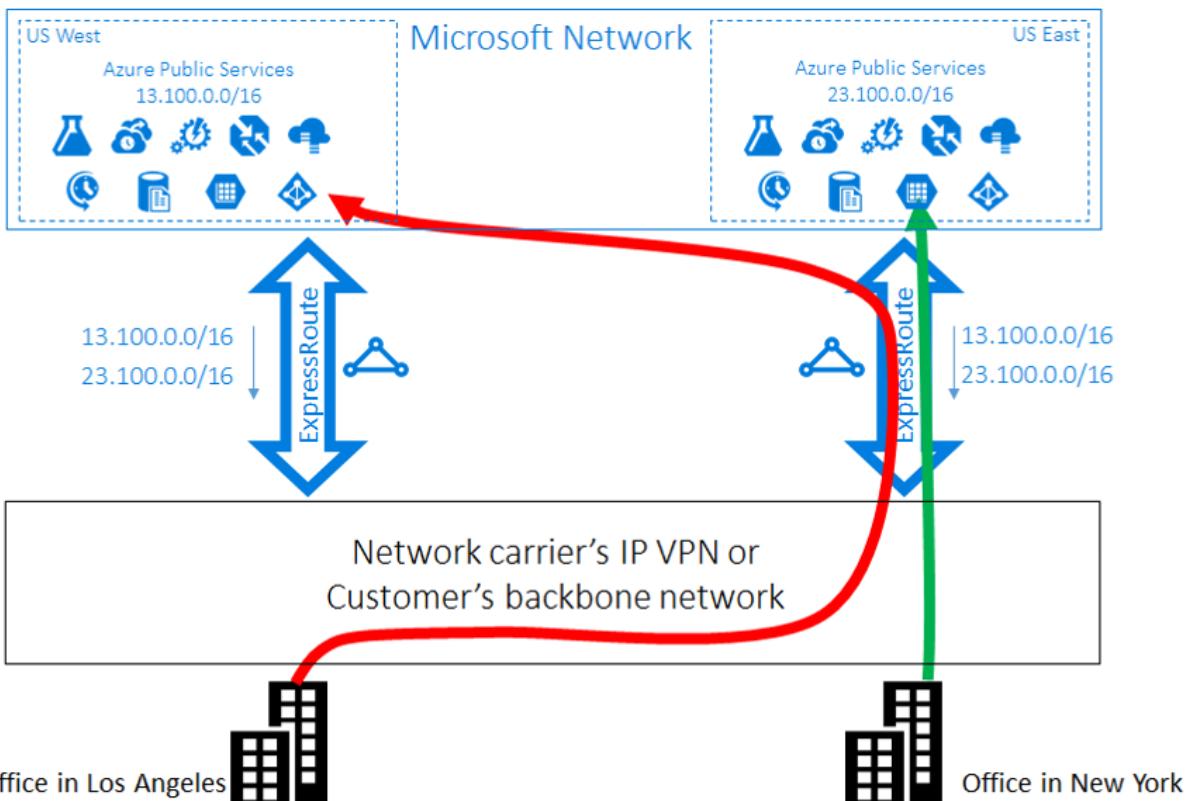


Figure 6: BGP communities unoptimized connection.

### Solution:

To optimize routing for both offices, you need to know which prefix is from Azure `West US` and which is from Azure `East US`. You can encode this information by using BGP community values.

- You assign a unique BGP community value to each Azure region. For example, 12076:51004 for **East US** ; 12076:51006 for **West US** .
- Now that it's clear which prefix belongs to which Azure region, you can configure a preferred ExpressRoute circuit.
- Because you're using BGP to exchange routing information, you can use BGP's local preference to influence routing.
- In our example, you assign a higher local preference value to **13.100.0.0/16** in **West us** than in **East US** . Similarly, you assign a higher local preference value to **23.100.0.0/16** in **East us** than in **West us** .
- This configuration ensures that when both paths to Microsoft are available, users in Los Angeles connect to the **West us** region by using the west circuit, and users in New York connect to the **East us** region by using the east circuit.

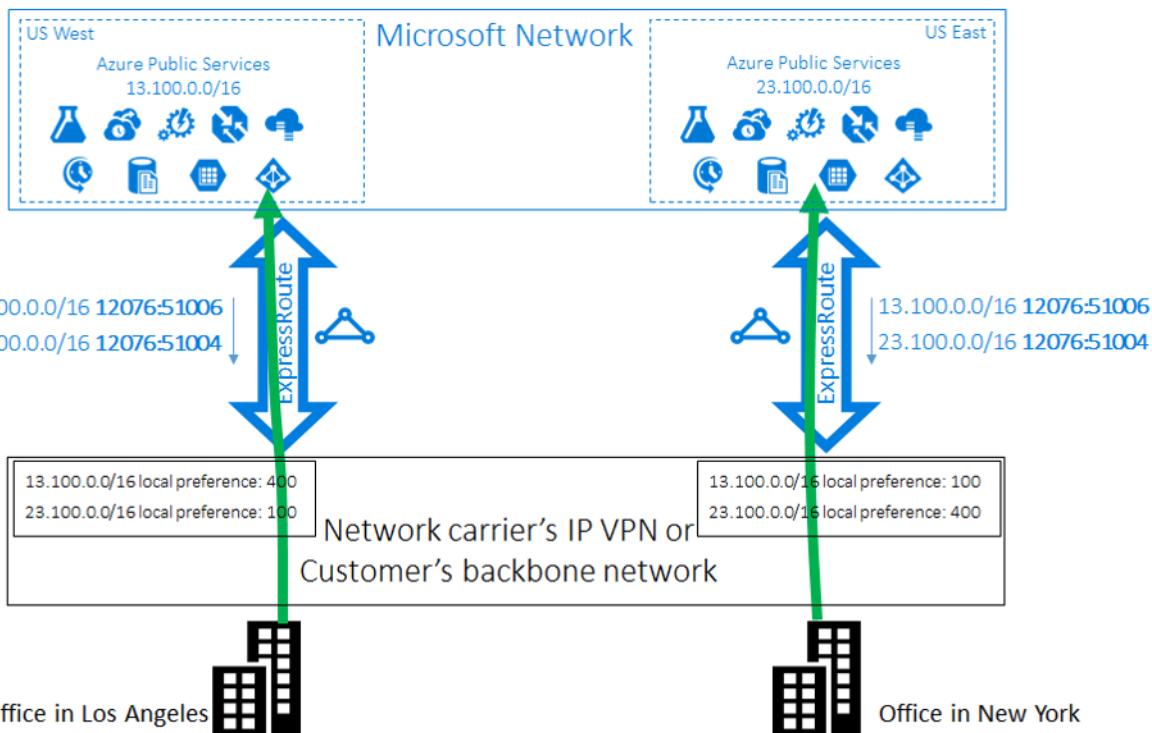


Figure 7: BGP communities optimized connection.

#### Learn more:

- Learn about [optimizing routing](#).

## Secure virtual networks

The responsibility for securing virtual networks is shared between Microsoft and you. Microsoft provides many networking features, as well as services that help keep resources secure. When you're designing security for virtual networks, it's best to implement a perimeter network, use filtering and security groups, secure access to resources and IP addresses, and implement attack protection.

#### Learn more:

- Read an [overview of best practices for network security](#).
- Learn how to [design for secure networks](#).

## Best practice: Implement an Azure perimeter network

Although Microsoft invests heavily in protecting the cloud infrastructure, you must also protect your cloud

services and resource groups. A multilayered approach to security provides the best defense. Putting a perimeter network in place is an important part of that defense strategy.

- A perimeter network protects internal network resources from an untrusted network.
- It's the outermost layer that's exposed to the internet. It generally sits between the internet and the enterprise infrastructure, usually with some form of protection on both sides.
- In a typical enterprise network topology, the core infrastructure is heavily fortified at the perimeters, with multiple layers of security devices. The boundary of each layer consists of devices and policy enforcement points.
- Each layer can include a combination of the network security solutions, such as firewalls, denial of service (DoS) prevention, intrusion detection/intrusion protection systems (IDS/IPS), and VPN devices.
- Policy enforcement on the perimeter network can use firewall policies, access control lists (ACLs), or specific routing.
- As incoming traffic arrives from the internet, it's intercepted and handled by a combination of defense solutions. The solutions block attacks and harmful traffic, while allowing legitimate requests into the network.
- Incoming traffic can route directly to resources in the perimeter network. The perimeter network resource can then communicate with other resources deeper in the network, moving traffic forward into the network after validation.

Here's an example of a single subnet perimeter network in a corporate network, with two security boundaries.

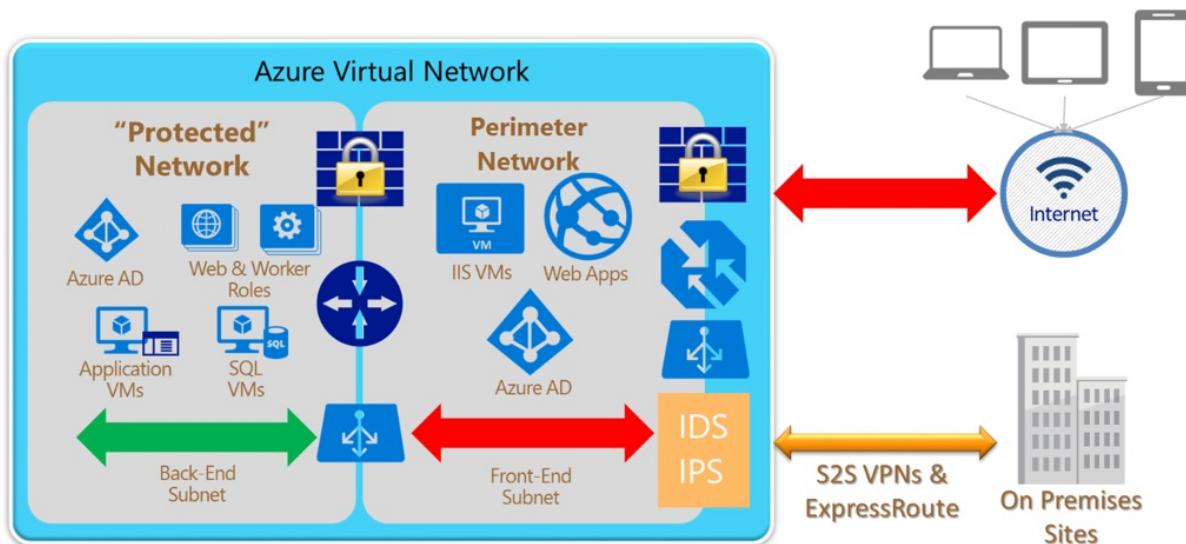


Figure 8: Perimeter network deployment.

#### Learn more:

- Learn how to deploy a perimeter network between Azure and your on-premises datacenter.

## Best practice: Filter virtual network traffic with NSGs

Network security groups (NSGs) contain multiple inbound and outbound security rules that filter traffic going to and from resources. Filtering can be by source and destination IP address, port, and protocol.

- NSGs contain security rules that allow or deny inbound network traffic to (or outbound network traffic from) several types of Azure resources. For each rule, you can specify source and destination, port, and protocol.
- NSG rules are evaluated by priority by using five-tuple information (source, source port, destination, destination port, and protocol), to allow or deny the traffic.
- A flow record is created for existing connections. Communication is allowed or denied based on the connection state of the flow record.
- A flow record allows an NSG to be stateful. For example, if you specify an outbound security rule to any address

over port 80, you don't need an inbound security rule to respond to the outbound traffic. You only need to specify an inbound security rule if communication is initiated externally.

- The opposite is also true. If inbound traffic is allowed over a port, you don't need to specify an outbound security rule to respond to traffic over the port.
- Existing connections aren't interrupted when you remove a security rule that enabled the flow. Traffic flows are interrupted when connections are stopped, and no traffic is flowing in either direction, for at least a few minutes.
- When creating NSGs, create as few as possible, but as many as necessary.

### Best practice: Secure north/south and east/west traffic

To secure virtual networks, consider attack vectors. Note the following points:

- Using only subnet NSGs simplifies your environment, but only secures traffic into your subnet. This is known as north/south traffic.
- Traffic between VMs on the same subnet is known as east/west traffic.
- It's important to use both forms of protection, so that if a hacker gains access from the outside, they'll be stopped when trying to attack machines located in the same subnet.

### Use service tags on NSGs

A service tag represents a group of IP address prefixes. Using a service tag helps minimize complexity when you create NSG rules.

- You can use service tags instead of specific IP addresses when you create rules.
- Microsoft manages the address prefixes associated with a service tag, and automatically updates the service tag as addresses change.
- You can't create your own service tag, or specify which IP addresses are included within a tag.

Service tags take the manual work out of assigning a rule to groups of Azure services. For example, if you want to allow a subnet containing web servers to access to Azure SQL Database, you can create an outbound rule to port 1433, and use the **Sql** service tag.

- This **Sql** tag denotes the address prefixes of the Azure SQL Database and Azure SQL Data Warehouse services.
- If you specify **Sql** as the value, traffic is allowed or denied to SQL.
- If you only want to allow access to **Sql** in a specific region, you can specify that region. For example, if you want to allow access only to Azure SQL Database in the East US region, you can specify **Sql.EastUS** for the service tag.
- The tag represents the service, but not specific instances of the service. For example, the tag represents the Azure SQL Database service, but doesn't represent a particular SQL Database or server.
- All address prefixes represented by this tag are also represented by the **Internet** tag.

Learn more:

- Read about [network security groups \(NSGs\)](#).
- Review the [service tags available for NSGs](#).

### Best practice: Use application security groups

Application security groups enable you to configure network security as a natural extension of an application structure.

- You can group VMs and define network security policies based on application security groups.
- Application security groups enable you to reuse your security policy at scale, without manual maintenance of explicit IP addresses.
- Application security groups handle the complexity of explicit IP addresses and multiple rule sets, allowing you

to focus on your business logic.

Example:

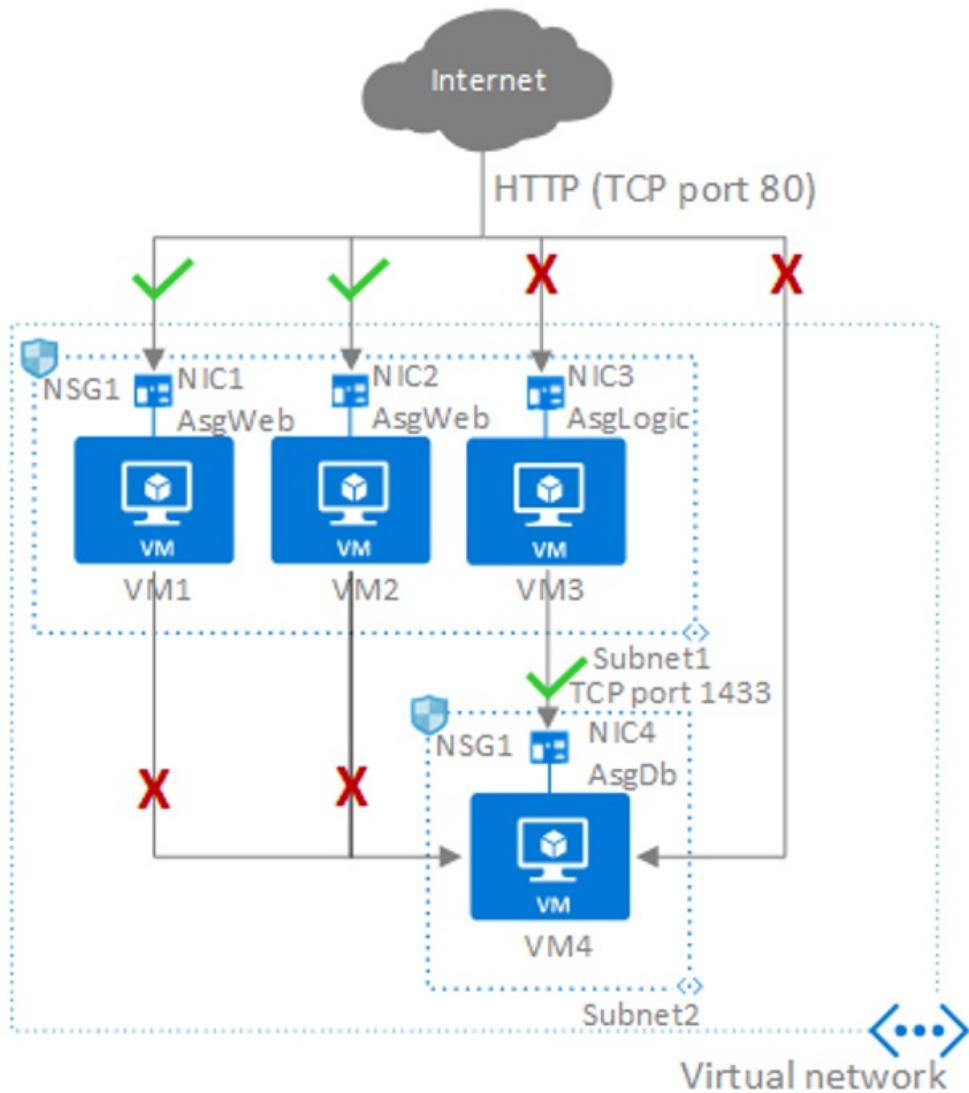


Figure 9:

Application security group example.

NETWORK INTERFACE	APPLICATION SECURITY GROUP
NIC1	AsgWeb
NIC2	AsgWeb
NIC3	AsgLogic
NIC4	AsgDb

In our example, each network interface belongs to only one application security group, but in fact an interface can belong to multiple groups, in accordance with Azure limits. None of the network interfaces have an associated NSG. NSG1 is associated with both subnets, and contains the following rules:

RULE NAME	PURPOSE	DETAILS

Rule Name	Purpose	Details
<code>Allow-HTTP-Inbound-Internet</code>	<p>Allow traffic from the internet to the web servers. Inbound traffic from the internet is denied by the <code>DenyAllInbound</code> default security rule, so no additional rule is needed for the <code>AsgLogic</code> or <code>AsgDb</code> application security groups.</p>	<p>Priority: <code>100</code>  Source: <code>internet</code>  Source port: <code>*</code>  Destination: <code>AsgWeb</code>  Destination port: <code>80</code>  Protocol: <code>TCP</code>  Access: <code>Allow</code></p>
<code>Deny-Database-All</code>	<p><code>AllowVNetInBound</code> default security rule allows all communication between resources in the same virtual network. This rule is needed to deny traffic from all resources.</p>	<p>Priority: <code>120</code>  Source: <code>*</code>  Source port: <code>*</code>  Destination: <code>AsgDb</code>  Destination port: <code>1433</code>  Protocol: <code>All</code>  Access: <code>Deny</code></p>
<code>Allow-Database-BusinessLogic</code>	<p>Allow traffic from the <code>AsgLogic</code> application security group to the <code>AsgDb</code> application security group. The priority for this rule is higher than the <code>Deny-Database-All</code> rule, so this rule is processed first. Therefore, traffic from the <code>AsgLogic</code> application security group is allowed, and all other traffic is blocked.</p>	<p>Priority: <code>110</code>  Source: <code>AsgLogic</code>  Source port: <code>*</code>  Destination: <code>AsgDb</code>  Destination port: <code>1433</code>  Protocol: <code>TCP</code>  Access: <code>Allow</code></p>

The rules that specify an application security group as the source or destination are only applied to the network interfaces that are members of the application security group. If the network interface isn't a member of an application security group, the rule is not applied to the network interface, even though the network security group is associated with the subnet.

#### Learn more:

- Learn about [application security groups](#).

#### Best practice: Secure access to PaaS by using virtual network service endpoints

Virtual network service endpoints extend your virtual network private address space and identity to Azure services over a direct connection.

- Endpoints allow you to secure critical Azure service resources to your virtual networks only. Traffic from your virtual network to the Azure service always remains on the Azure backbone network.

- Virtual network private address space can be overlapping, and thus can't be used to uniquely identify traffic originating from a virtual network.
- After you enable service endpoints in your virtual network, you can secure Azure service resources by adding a virtual network rule to the service resources. This provides improved security by fully removing public internet access to resources, and allowing traffic only from your virtual network.

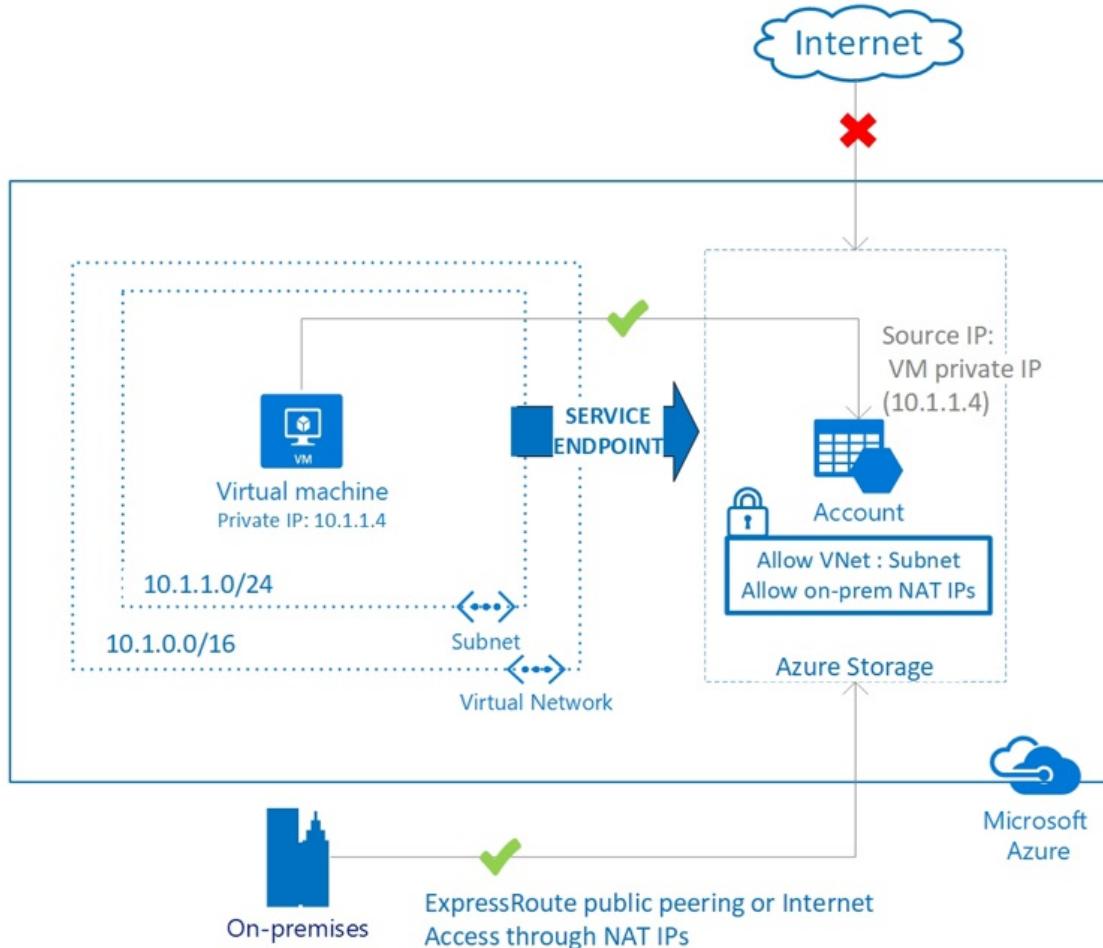


Figure 10: Service endpoints.

#### Learn more:

- Learn about [virtual network service endpoints](#).

## Best practice: Control public IP addresses

Public IP addresses in Azure can be associated with VMs, load balancers, application gateways, and VPN gateways.

- Public IP addresses allow internet resources to communicate inbound to Azure resources, and Azure resources to communicate outbound to the internet.
- Public IP addresses are created with a basic or Standard SKU, which have several differences. Standard SKUs can be assigned to any service, but are most usually configured on VMs, load balancers, and application gateways.
- It's important to note that a basic public IP address doesn't have an NSG automatically configured. You need to configure your own, and assign rules to control access. Standard SKU IP addresses have an NSG, and rules assigned by default.
- As a best practice, VMs shouldn't be configured with a public IP address.
  - If you need a port opened, it should only be for web services, such as port 80 or 443.
  - Standard remote management ports, such as SSH (22) and RDP (3389), along with all other ports,

should be set to deny by using NSGs.

- A better practice is to put VMs behind Azure Load Balancer or Azure Application Gateway. Then, if you need access to remote management ports, you can use just-in-time VM access in Azure Security Center.

#### Learn more:

- [Public IP addresses in Azure](#)
- [Manage virtual machine access by using just-in-time](#)

## Take advantage of Azure security features for networking

Azure has platform-level security features, including Azure Firewall, Web Application Firewall, and Network Watcher.

### Best practice: Deploy Azure Firewall

Azure Firewall is a managed, cloud-based, network security service that helps protect your virtual network resources. It's a fully stateful, managed firewall, with built-in high availability and unrestricted cloud scalability.

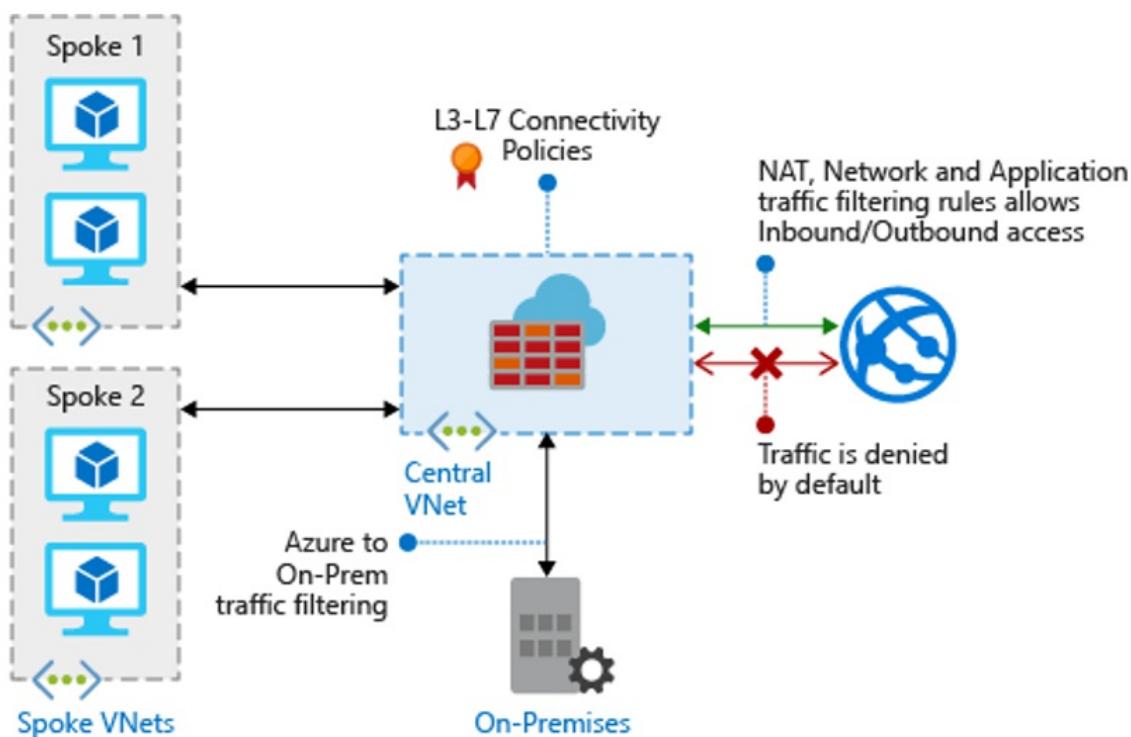


Figure 11: Azure Firewall.

Here are a few points to be aware of if you deploy the service:

- Azure Firewall can centrally create, enforce, and log application and network connectivity policies across subscriptions and virtual networks.
- Azure Firewall uses a static, public IP address for your virtual network resources. This allows outside firewalls to identify traffic originating from your virtual network.
- Azure Firewall is fully integrated with Azure Monitor for logging and analytics.
- When you're creating Azure Firewall rules, it's best to use the FQDN tags.
  - An FQDN tag represents a group of FQDNs associated with well-known Microsoft services.
  - You can use an FQDN tag to allow the required outbound network traffic through the firewall.
- For example, to manually allow Windows Update network traffic through your firewall, you would need to create multiple application rules. By using FQDN tags, you create an application rule, and include the Windows Update tag. With this rule in place, network traffic to Microsoft Windows Update endpoints can flow through

your firewall.

**Learn more:**

- Read the [Azure Firewall overview](#).
- Learn about [FQDN tags in Azure Firewall](#).

## Best practice: Deploy Web Application Firewall

Web applications are increasingly targets of malicious attacks that exploit commonly known vulnerabilities. Exploits include SQL injection attacks and cross-site scripting attacks. Preventing such attacks in application code can be challenging, and can require rigorous maintenance, patching, and monitoring at multiple layers of the application topology.

Web Application Firewall (WAF), a feature of Azure Application Gateway, helps make security management much simpler, and helps application administrators guard against threats or intrusions. You can react to security threats faster, by patching known vulnerabilities at a central location, instead of securing individual web applications. You can easily convert existing application gateways to Application Gateway that is enabled for Web Application Firewall.

Here are some additional notes about WAF:

- WAF provides centralized protection of your web applications from common exploits and vulnerabilities.
- You don't need to modify your code to make use of WAF.
- It can protect multiple web apps at the same time, behind Application Gateway.
- WAF is integrated with Azure Security Center.
- You can customize WAF rules and rule groups to suit your application requirements.
- As a best practice, you should use a WAF in front of any web-facing application, including applications on Azure VMs or in Azure App Service.

**Learn more:**

- Learn about [WAF](#).
- Review [WAF limitations and exclusions](#).

## Best practice: Implement Azure Network Watcher

Azure Network Watcher provides tools to monitor resources and communications in an Azure virtual network. For example, you can monitor communications between a VM and an endpoint, such as another VM or FQDN. You can also view resources and resource relationships in a virtual network, or diagnose network traffic issues.

The screenshot shows the Network Watcher - NSG flow logs interface. On the left, there's a navigation sidebar with sections like Overview, MONITORING (Topology), NETWORK DIAGNOSTIC TOOLS (IP flow verify, Next hop, Security group view, Packet capture), METRICS (Network subscription limit), and LOGS (NSG flow logs, Diagnostic logs). The 'NSG flow logs' option is selected. The main area has a search bar at the top and filters for Subscription (Microsoft Azure), Resource group, Resource type, and Resource. A message says 'You can download flow logs from configured storage accounts.' Below is a table with columns: NAME, RESOURCE TYPE, RESOURCE GROUP, STATUS, and STORAGE ACCOUNT. The table lists several NSGs:

NAME	RESOURCE TYPE	RESOURCE GROUP	STATUS	STORAGE ACCOUNT
webtestnsg-c3dxj32iloqq-	Network security group	ContosoAppGateway	Disabled	
webtestnsg-h7frpjib4hd--	Network security group	ContosoAppGateway	Enabled	webtestvhdc3dxj32iloqqo
fabrikmvm1-nsg	Network security group	FabrikamRG	Disabled	
fabrikmvm3-nsg	Network security group	FabrikamRG	Enabled	webtestvhdc3dxj32iloqqo
fabrikmvm4-nsg	Network security group	FabrikamRG	Disabled	
webtestnsg-r5wpjct4pltz--	Network security group	testresourcegroup	Disabled	
webtestnsg-xqpow6s7bp--	Network security group	testresourcegroup	Disabled	

Figure 12: Network Watcher.

Here are a few more details:

- With Network Watcher, you can monitor and diagnose networking issues without signing into VMs.
- You can trigger packet capture by setting alerts, and gain access to real-time performance information at the packet level. When you see an issue, you can investigate it in detail.
- As a best practice, use Network Watcher to review NSG flow logs.
  - NSG flow logs in Network Watcher allow you to view information about ingress and egress IP traffic through an NSG.
  - Flow logs are written in JSON format.
  - Flow logs show outbound and inbound flows on a per-rule basis, and the network interface (NIC) to which the flow applies. They also show 5-tuple information about the flow (source/destination IP, source/destination port, and protocol), and whether the traffic was allowed or denied.

#### Learn more:

- Read the [Network Watcher overview](#).
- Learn more about [NSG flow logs](#).

## Use partner tools in Azure Marketplace

For more complex network topologies, you might use security products from Microsoft partners, in particular network virtual appliances (NVAs).

- An NVA is a VM that performs a network function, such as a firewall, WAN optimization, or other network function.
- NVAs bolster virtual network security and network functions. They can be deployed for highly available firewalls, intrusion prevention, intrusion detection, WAFs, WAN optimization, routing, load balancing, VPN, certificate management, Active Directory, and multi-factor authentication.
- NVAs are available from numerous vendors in [Azure Marketplace](#).

## Best practice: Implement firewalls and NVAs in hub networks

In the hub, you normally manage the perimeter network (with access to the internet) through Azure Firewall, a firewall farm, or a WAF. The following table provides comparisons of these.

FIREWALL TYPE	DETAILS
WAFs	Web applications are common, and tend to suffer from vulnerabilities and potential exploits. WAFs are designed to detect attacks against web applications (HTTP/HTTPS). Compared with traditional firewall technology, WAFs have a set of specific features that protect internal web servers from threats.
Azure Firewall	Like NVA firewall farms, Azure Firewall uses a common administration mechanism and a set of security rules to protect workloads hosted in spoke networks. Azure Firewall also helps control access to on-premises networks. Azure Firewall has built-in scalability.
NVA firewalls	<p>Like Azure Firewall, NVA firewall farms have a common administration mechanism and a set of security rules to protect workloads hosted in spoke networks. NVA firewalls also help control access to on-premises networks. NVA firewalls can be manually scaled behind a load balancer.</p> <p>Though an NVA firewall has less specialized software than a WAF, it has broader application scope to filter and inspect any type of traffic in egress and ingress.</p>

We recommend using one set of Azure firewalls (or NVAs) for traffic originating on the internet, and another for traffic originating on-premises. Using only one set of firewalls for both is a security risk, as it provides no security perimeter between the two sets of network traffic. Using separate firewall layers reduces the complexity of checking security rules, and it's clear which rules correspond to which incoming network request.

#### Learn more:

- Learn about [using NVAs in an Azure Virtual Network](#).

## Next steps

Review other best practices:

- [Best practices](#) for security and management after migration.
- [Best practices](#) for cost management after migration.

# Deploy a migration infrastructure

11/9/2020 • 38 minutes to read • [Edit Online](#)

This article shows how the fictional company Contoso prepares its on-premises infrastructure for migration, sets up an Azure infrastructure in preparation for migration, and runs the business in a hybrid environment.

When you use this example to help plan your own infrastructure migration efforts, keep in mind that the provided sample architecture is specific to Contoso. Review your organization's business needs, structure, and technical requirements when making important infrastructure decisions about subscription design or network architecture.

Whether you need all the elements described in this article depends on your migration strategy. For example, you might need a less complex network structure if you're building only cloud-native applications in Azure.

## Overview

Before Contoso can migrate to Azure, it's critical to prepare an Azure infrastructure. Generally, Contoso needs to think about six areas:

- **Step 1: Azure subscriptions.** How will it purchase Azure and interact with the Azure platform and services?
- **Step 2: Hybrid identity.** How will it manage and control access to on-premises and Azure resources after migration? How does it extend or move identity management to the cloud?
- **Step 3: Disaster recovery and resilience.** How will it ensure that its applications and infrastructure are resilient if outages and disasters occur?
- **Step 4: Network.** How should it design a network infrastructure and establish connectivity between its on-premises datacenter and Azure?
- **Step 5: Security.** How will it secure the hybrid deployment?
- **Step 6: Governance.** How will it keep the deployment aligned with security and governance requirements?

## Before you start

Before we start reviewing the infrastructure, consider reading some background information about relevant Azure capabilities:

- Several options are available for purchasing Azure access, including pay-as-you-go subscriptions, a Microsoft Enterprise Agreement (EA), Open Licensing from Microsoft resellers, or purchasing from Microsoft partners in the Cloud Solution Provider (CSP) program. Learn about [purchase options](#), and read about how [Azure subscriptions are organized](#).
- Get an overview of Azure [identity and access management \(IAM\)](#). Learn about [Azure Active Directory \(Azure AD\)](#) and [extending on-premises Active Directory to the cloud](#).
- Azure provides a robust network infrastructure with options for hybrid connectivity. Get an overview of [networking and network access control](#).
- Read the [introduction to Azure security](#) and learn how to create a plan for [Azure governance](#).

## On-premises architecture

Here's a diagram that shows the current Contoso on-premises infrastructure.

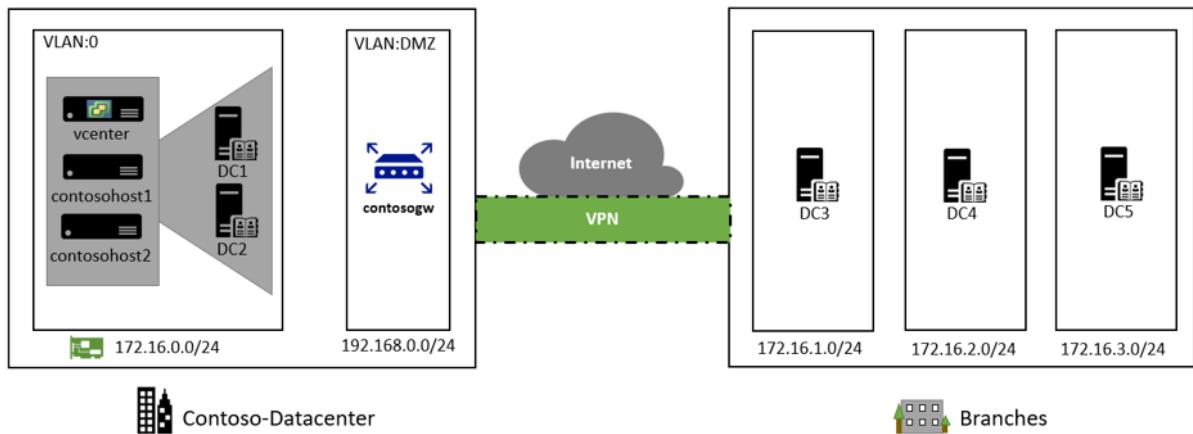


Figure 1: Contoso on-premises architecture.

- Contoso has one main datacenter located in New York City in the eastern United States.
- There are three additional local branches across the United States.
- The main datacenter is connected to the internet with a fiber-optic Metro Ethernet connection (500 Mbps).
- Each branch is connected locally to the internet through business-class connections, with IPsec VPN tunnels back to the main datacenter. This approach allows the entire network to be permanently connected and optimizes internet connectivity.
- The main datacenter is fully virtualized with VMware. Contoso has two ESXi 6.5 virtualization hosts managed by vCenter Server 6.5.
- Contoso uses Active Directory for identity management and domain name system (DNS) servers on the internal network.
- The domain controllers in the datacenter run on VMware virtual machines (VMs). The domain controllers at local branches run on physical servers.

## Step 1: Buy and subscribe to Azure

Contoso needs to figure out how to buy Azure, how to manage subscriptions, and how to license services and resources.

### Buy Azure

Contoso is enrolling in an [Enterprise Agreement](#). This agreement entails an upfront monetary commitment to Azure. It entitles Contoso to earn benefits like flexible billing options and optimized pricing.

Here are the details:

- Contoso estimated what its yearly Azure spend will be. When it signed the agreement, Contoso paid for the first year in full.
- Contoso needs to use all commitments before the year is over or lose the value for those dollars.
- If for some reason Contoso exceeds its commitment and spends more, Microsoft will invoice for the difference.
- Any cost incurred above the commitment will be at the same rates as those in the Contoso contract. There are no penalties for going over.

### Manage subscriptions

After paying for Azure, Contoso needs to figure out how to manage Azure subscriptions. Because Contoso has an EA, there's no limit on the number of Azure subscriptions it can create. An Azure Enterprise Agreement enrollment defines how a company shapes and uses Azure services, and defines a core governance structure.

As a first step, Contoso has defined a structure known as an *enterprise scaffold* for its enrollment. Contoso

used the [Azure enterprise scaffold guidance](#) to help understand and design a scaffold.

For now, Contoso has decided to use a functional approach to manage subscriptions:

- Inside the enterprise, it will use a single IT department that controls the Azure budget. This will be the only group with subscriptions.
- Contoso will extend this model in the future, so that other corporate groups can join as departments in the enrollment hierarchy.
- Inside the IT department, Contoso has structured two subscriptions, `Production` and `Development`.
- If Contoso needs more subscriptions in the future, it will also need to manage access, policies, and compliance for those subscriptions. Contoso will do that by introducing [Azure management groups](#) as an additional layer above subscriptions.

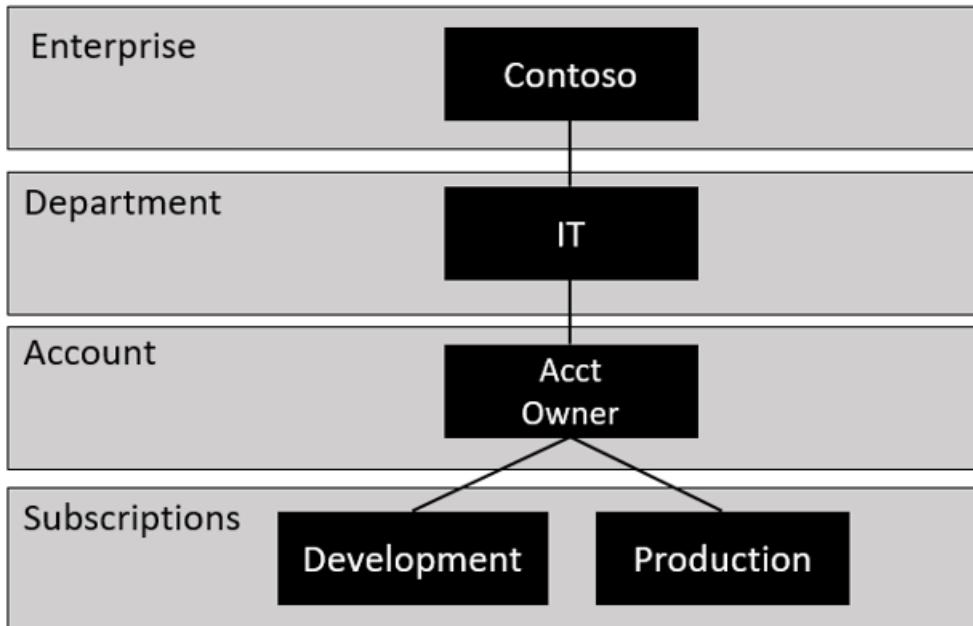


Figure 2: Enterprise hierarchy.

### Examine licensing

With subscriptions configured, Contoso can look at Microsoft licensing. The licensing strategy will depend on the resources that Contoso wants to migrate to Azure and how VMs and services are selected and deployed in Azure.

#### Azure Hybrid Benefit

For deploying VMs in Azure, standard images include a license that will charge Contoso by the minute for the software being used. However, Contoso has been a long-term Microsoft customer and has maintained EAs and open licenses with Software Assurance.

Azure Hybrid Benefit provides a cost-effective method for migration. It allows Contoso to save on Azure VMs and SQL Server workloads by converting or reusing Windows Server Datacenter and Standard edition licenses covered with Software Assurance. This allows Contoso to pay a lower base compute rate for VMs and SQL Server. For more information, see [Azure Hybrid Benefit](#).

#### License Mobility

License Mobility through Software Assurance gives Microsoft Volume Licensing customers like Contoso the flexibility to deploy eligible server applications with active Software Assurance on Azure. This eliminates the need to purchase new licenses. With no associated mobility fees, existing licenses can easily be deployed in Azure. For more information, see [License Mobility through Software Assurance on Azure](#).

#### Reserved instances for predictable workloads

Predictable workloads always need to be available with VMs running, such as line-of-business applications

like an SAP ERP system. Unpredictable workloads are variable, like VMs that are on during high demand and off when demand is low.

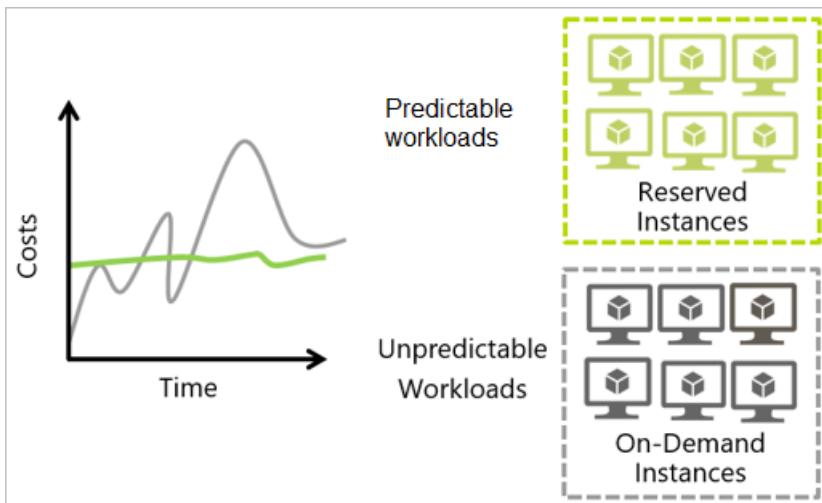


Figure 3: Azure Reserved Virtual Machine Instances.

In exchange for using reserved instances for specific VM instances that must be maintained for long durations, Contoso can get both a discount and prioritized capacity. Using [Azure Reserved Virtual Machine Instances](#) together with Azure Hybrid Benefit can save Contoso up to 82 percent off regular pay-as-you-go pricing (as of April 2018).

## Step 2: Manage hybrid identity

Giving and controlling user access to Azure resources with identity and access management is an important step in pulling together an Azure infrastructure.

Contoso decides to extend its on-premises Active Directory into the cloud, rather than build a new separate system in Azure. Because Contoso isn't using Microsoft 365 yet, it needs to provision an Azure AD instance. If Contoso were using Microsoft 365, it would already have an existing Azure AD tenant and directory, which it could use as its primary Azure AD instance.

Learn more about [Microsoft 365 identity models and Azure Active Directory](#). You can also learn how to [associate or add an Azure subscription to your Azure Active Directory tenant](#).

### Create an Azure AD directory

Contoso is using the Azure AD Free edition that's included with an Azure subscription. Contoso admins create an Azure AD directory:

1. In the [Azure portal](#), they go to **Create a resource > Identity > Azure Active Directory**.
2. In **Create directory**, they specify a name for the directory, an initial domain name, and the region where the directory should be created.

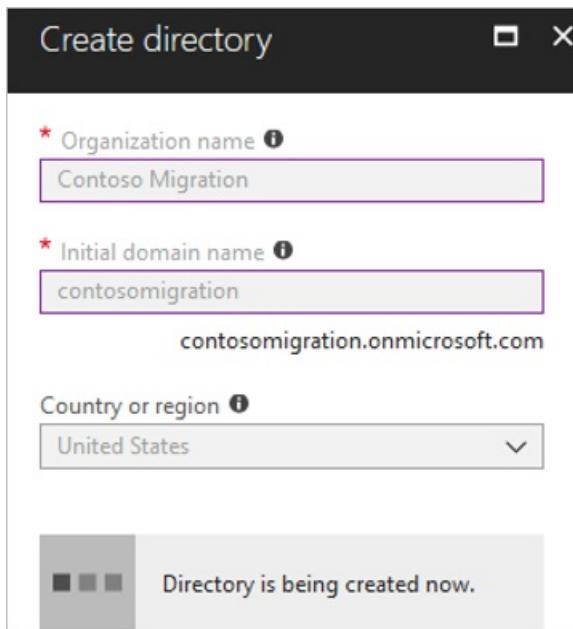


Figure 4: Create an Azure AD directory.

#### NOTE

The directory that's created has an initial domain name in the form `domain-name.onmicrosoft.com`. The name can't be changed or deleted. Instead, the admins need to add its registered domain name to Azure AD.

#### Add the domain name

To use the standard domain name, Contoso admins need to add it as a custom domain name to Azure AD. This option allows them to assign familiar user names. For example, a user can sign in with the email address `billg@contoso.com` instead of `billg@contosomigration.onmicrosoft.com`.

To set up a custom domain name, the admins add it to the directory, add a DNS entry, and then verify the name in Azure AD.

1. In **Custom domain names > Add custom domain**, they add the domain.
2. To use a DNS entry in Azure, they need to register it with their domain registrar:
  - In the **Custom domain names** list, they note the DNS information for the name. It's using an MX record.
  - They need access to the name server. They log in to the `contoso.com` domain and create a new MX record for the DNS entry provided by Azure AD, by using the details noted.
3. After the DNS records propagate, they select **Verify** to check the custom domain name in the details for the domain.

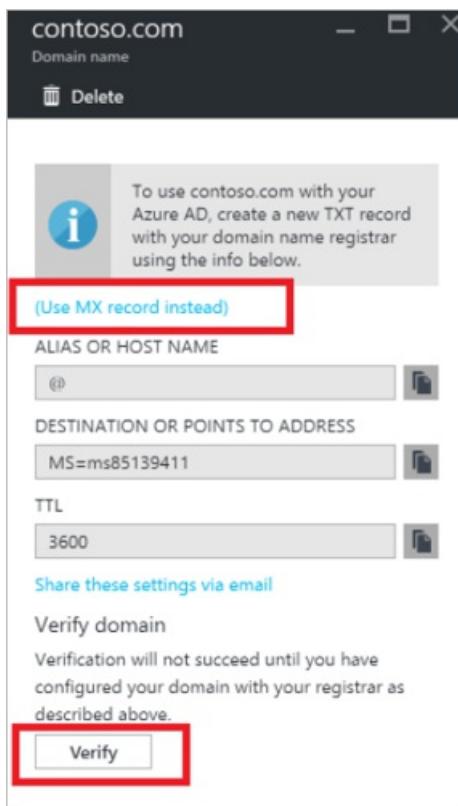


Figure 5: Checking the domain name.

## Set up on-premises and Azure groups and users

Now that the Azure AD directory is established, Contoso admins need to add employees to on-premises Active Directory groups that will synchronize to Azure AD. They should use on-premises group names that match the names of resource groups in Azure. This makes it easier to identify matches for synchronization purposes.

### Create resource groups in Azure

Azure resource groups gather Azure resources together. Using a resource group ID allows Azure to perform operations on the resources within the group.

An Azure subscription can have multiple resource groups. A resource group exists in a single subscription. In addition, a single resource group can have multiple resources. A resource belongs to a single resource group.

Contoso admins set up Azure resource groups as shown in the following table.

RESOURCE GROUP	DETAILS
ContosoCobRG	This group contains all resources related to continuity of business. It includes vaults that Contoso will use for the Azure Site Recovery service and the Azure Backup service. It also includes resources used for migration, including Azure Migrate and Azure Database Migration Service.
ContosoDevRG	This group contains dev/test resources.
ContosoFailoverRG	This group serves as a landing zone for failed-over resources.
ContosoNetworkingRG	This group contains all network resources.

RESOURCE GROUP	DETAILS
ContosoRG	This group contains resources related to production applications and databases.

They create resource groups as follows:

1. In the Azure portal > **Resource groups**, they add a group.
2. For each group, they specify a name, the subscription to which the group belongs, and the region.
3. Resource groups appear in the **Resource groups** list.

The screenshot shows the 'Resource groups' blade in the Azure portal. At the top, there's a search bar containing 'contoso'. Below it, a table lists six resource groups:

NAME
ContosoCobRG
ContosoDevRG
ContosoFailoverRG
ContosoInfraRG
ContosoNetworkingRG
ContosoRG

Figure 6: Resource groups.

#### Scale resource groups

In future, Contoso will add other resource groups based on needs. For example, it might define a resource group for each application or service so that each can be managed and secured independently.

#### Create matching security groups on-premises

In the on-premises Active Directory instance, Contoso admins set up security groups with names that match the names of the Azure resource groups.

The screenshot shows the 'Active Directory Administrative Center' interface. On the left, the navigation pane shows 'contoso (local) > ContosoGroups (7)'. The main pane displays a table of security groups:

Name	Type	Description
ContosoAzureAdmins	Group	Azure Resource Group
ContosoCobRG	Group	Azure Resource Group
ContosoDevRG	Group	Azure Resource Group
ContosoFailoverRG	Group	Azure Resource Group
ContosoInfraRG	Group	Azure Resource Group
ContosoNetworkingRG	Group	Azure Resource Group
ContosoRG	Group	Azure Resource Group

Figure 7: On-premises Active Directory security groups.

For management purposes, they create an additional group that will be added to all of the other groups. This group will have rights to all resource groups in Azure. A limited number of global admins will be added to this group.

## Synchronize Active Directory

Contoso wants to provide a common identity for accessing resources on-premises and in the cloud. To do this, it will integrate the on-premises Active Directory instance with Azure AD. With this model, users and organizations can take advantage of a single identity to access on-premises applications and cloud services, such as Microsoft 365, or thousands of other sites on the internet. Admins can use the groups in Active Directory to implement [role-based access control \(RBAC\)](#) in Azure.

To facilitate integration, Contoso uses the [Azure AD Connect tool](#). When you install and configure the tool on a domain controller, it synchronizes the on-premises Active Directory identities to Azure AD.

### Download the tool

1. In the Azure portal, Contoso admins go to [Azure Active Directory > Azure AD Connect](#) and download the latest version of the tool to the server they're using for synchronization.

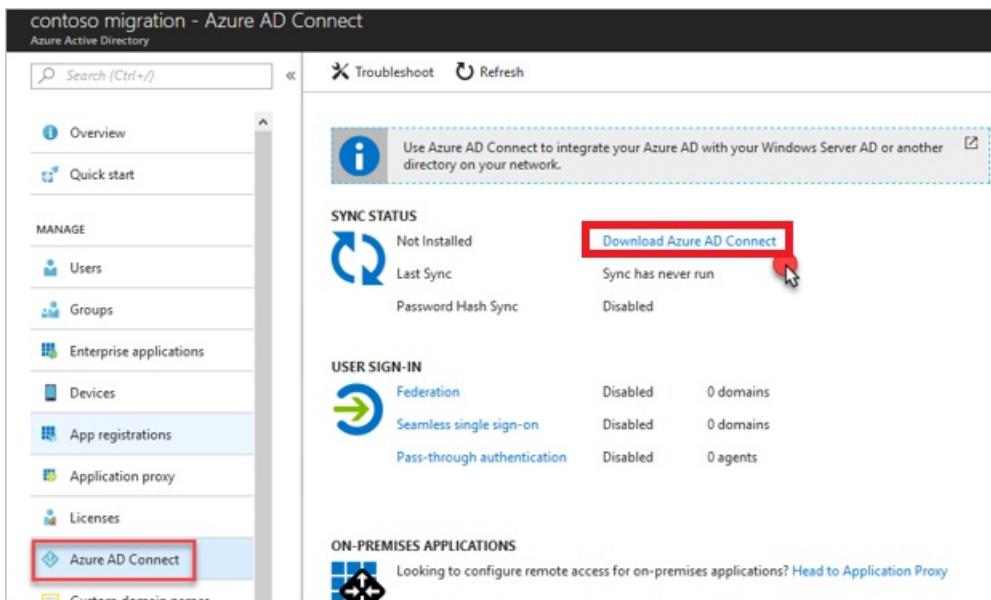


Figure 8: Downloading Azure AD Connect.

2. They start the `AzureADConnect.msi` installation by using [Express Settings](#). This is the most common installation, and it can be used for a single-forest topology with password-hash synchronization for authentication.

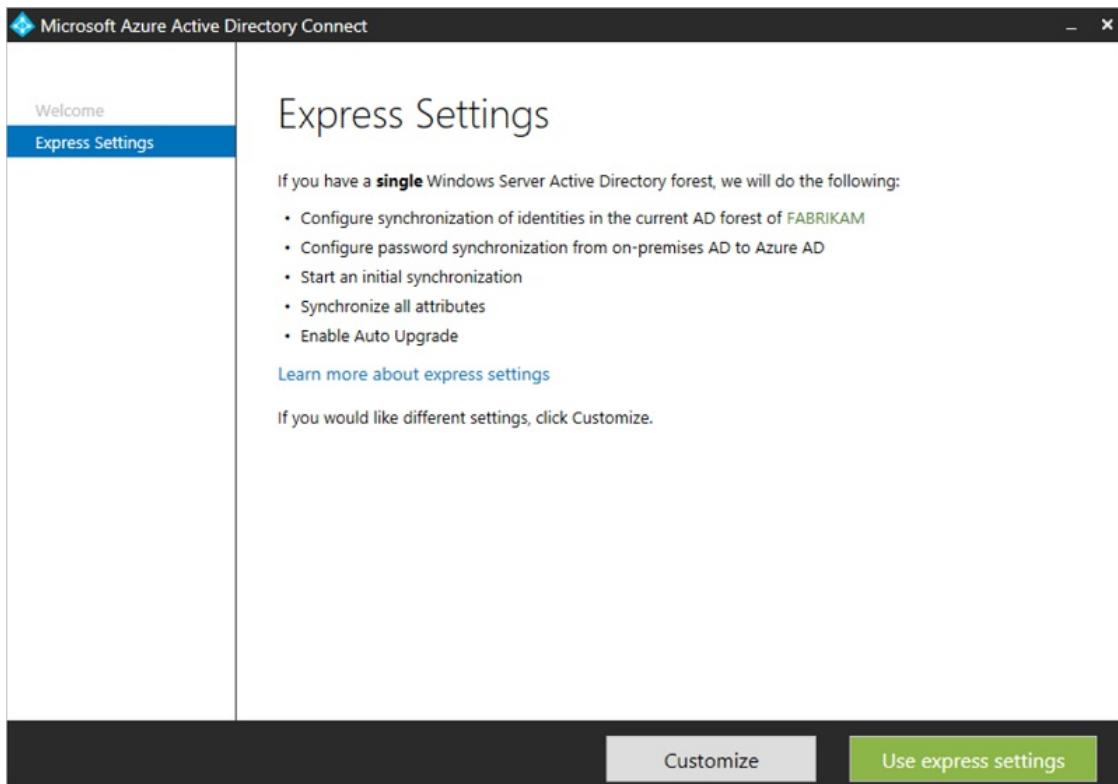


Figure 9: Azure AD Connect Wizard.

3. In **Connect to Azure AD**, they specify the credentials for connecting to Azure AD (in the form

`admin@contoso.com` or `admin@contoso.onmicrosoft.com` ).

This is a screenshot of the 'Connect to Azure AD' step. The title is 'Connect to Azure AD'. Below it, a placeholder text says 'Enter your Azure AD global administrator credentials.' followed by a question mark icon. There are two input fields: 'USERNAME' containing 'contosoadmin@contosomigration.onmicrosoft.com' and 'PASSWORD' containing a series of asterisks.

Figure 10: Azure AD Connect Wizard: Connect to Azure AD.

4. In **Connect to AD DS**, they specify credentials for the on-premises directory (in the form

`CONTOSO\admin` or `contoso.com\admin` ).

This is a screenshot of the 'Connect to AD DS' step. The title is 'Connect to AD DS'. Below it, a placeholder text says 'Enter the Active Directory Domain Services enterprise administrator credentials:' followed by a question mark icon. There are two input fields: 'USERNAME' containing 'CONTOSO.COM\administrator' and 'PASSWORD' containing a series of asterisks.

Figure 11: Azure AD Connect Wizard: Connect to AD DS.

5. In **Ready to configure**, they select **Start the synchronization process when configuration completes** to start the sync immediately. Then they install.

Note the following:

- Contoso has a direct connection to Azure. If your on-premises Active Directory instance is behind a proxy, review [troubleshoot Azure AD connectivity](#).

- After the first synchronization, on-premises Active Directory objects are visible in the Azure AD directory.

NAME
co ContosoAzureAdmins
co ContosoCobRG
co ContosoDevRG
co ContosoFailoverRG
co ContosoInfraRG
co ContosoNetworkingRG
co ContosoRG

Figure 12: On-premises Active Directory objects visible in Azure AD.

- The Contoso IT team is represented in each group and is based on its role.

NAME
CC Chad Corbitt
KT Kari Tran
WM Wade Munger
AB Abel Bevins
CO ContosoAzureAdmins

Figure 13: Group membership.

## Set up RBAC

Azure RBAC enables fine-grained access management for Azure. By using RBAC, you can grant only the amount of access that users need to perform tasks. You assign the appropriate RBAC role to users, groups, and applications at a scope level. The scope of a role assignment can be a subscription, a resource group, or

a single resource.

Contoso admins then assign roles to the Active Directory groups that they synchronized from on-premises.

1. In the **ControlCobRG** resource group, they select **Access control (IAM) > Add role assignment**.
2. In **Add role assignment > Role > Contributor**, they select the **ContosoCobRG** security group from the list. The group then appears in the **Selected members** list.
3. They repeat this with the same permissions for the other resource groups (except for **ContosoAzureAdmins**) by adding **Contributor** permissions to the security group that matches the resource group.
4. For the **ContosoAzureAdmins** security group, they assign the **Owner** role.

Name	contoso
NAME	ContosoAzureAdmins
CO	ContosoCobRG
CO	ContosoDevRG
CO	ContosoFailoverRG
CO	ContosoInfraRG
CO	ContosoNetworkingRG
CO	ContosoRG

Figure 14: Assigning roles to security groups.

## Step 3: Design for resiliency

### Set up regions

Azure resources are deployed within regions. Regions are organized into geographies. Data residency, sovereignty, compliance, and resiliency requirements are honored within geographical boundaries.

A region consists of a set of datacenters. These datacenters are deployed within a latency-defined perimeter, and connected through a dedicated regional low-latency network.

Each Azure region is paired with a different region for resiliency. Read about [Azure regions](#), and understand [how regions are paired](#).

Contoso has decided to use **East US 2** (located in Virginia) as the primary region and **Central US** (located in Iowa) as the secondary region, for these reasons:

- The Contoso datacenter is located in New York, and Contoso considered latency to the closest datacenter.

- **East US 2** has all the services and products that Contoso needs. Not all Azure regions have the same products and services available. For more information, see [Azure products by region](#).
- **Central US** is the Azure paired region for **East US 2**.

As it thinks about the hybrid environment, Contoso needs to consider how to build resilience and a disaster recovery strategy into the region design. The simplest strategy is a single-region deployment, which relies on Azure platform features such as fault domains and regional pairing for resilience. The most complex is a full active-active model in which cloud services and database are deployed and servicing users from two regions.

Contoso has decided to take a middle road. It will deploy applications and resources in a primary region and keep a full copy of the infrastructure in the secondary region. With that strategy, the copy is ready to act as a full backup if a complete application disaster or regional failure occurs.

## **Set up availability**

### **Availability sets**

Availability sets help protect applications and data from a local hardware and network outage within a datacenter. Availability sets distribute Azure VMs across physical hardware within a datacenter.

Fault domains represent underlying hardware with a common power source and network switch within the datacenter. VMs in an availability set are distributed across fault domains to minimize outages caused by a single hardware or network failure.

Update domains represent underlying hardware that can undergo maintenance or be rebooted at the same time. Availability sets also distribute VMs across multiple update domains to ensure that at least one instance will be running at all times.

Contoso will implement availability sets whenever VM workloads require high availability. For more information, see [Manage the availability of Windows VMs in Azure](#).

### **Availability Zones**

Availability Zones help protect applications and data from failures that affect an entire datacenter within a region.

Each Availability Zone represents a unique physical location within an Azure region. Each zone consists of one or more datacenters equipped with independent power, cooling, and networking.

There's a minimum of three separate zones in all enabled regions. The physical separation of zones within a region protects applications and data from datacenter failures.

Contoso will use Availability Zones whenever applications need greater scalability, availability, and resilience. For more information, see [Regions and Availability Zones in Azure](#).

## **Configure backup**

### **Azure Backup**

You can use Azure Backup to back up and restore Azure VM disks.

Azure Backup allows automated backups of VM disk images stored in Azure Storage. Backups are application consistent to ensure that backed-up data is transactionally consistent and that applications will start post-restore.

Azure Backup supports locally redundant storage (LRS) to replicate multiple copies of backup data within a datacenter if a local hardware failure occurs. If a regional outage occurs, Azure Backup also supports geo-redundant storage (GRS), which replicates backup data to a secondary paired region.

Azure Backup encrypts data in transit by using AES-256. Backed-up data at rest is encrypted through [Azure Storage encryption](#).

Contoso will use Azure Backup with GRS on all production VMs to ensure that workload data is backed up and can be quickly restored if a disruption occurs. For more information, see [An overview of Azure VM backup](#).

### Set up disaster recovery

#### Azure Site Recovery

Azure Site Recovery helps ensure business continuity by keeping business applications and workloads running during regional outages.

Azure Site Recovery continuously replicates Azure VMs from a primary to a secondary region, ensuring functional copies in both locations. In the event of an outage in the primary region, the application or service fails over to using the VM instances replicated in the secondary region. This failover minimizes potential disruption. When operations return to normal, the applications or services can fail back to VMs in the primary region.

Contoso will implement [Azure Site Recovery](#) for all production VMs used in mission-critical workloads, ensuring minimal disruption during an outage in the primary region.

## Step 4: Design a network infrastructure

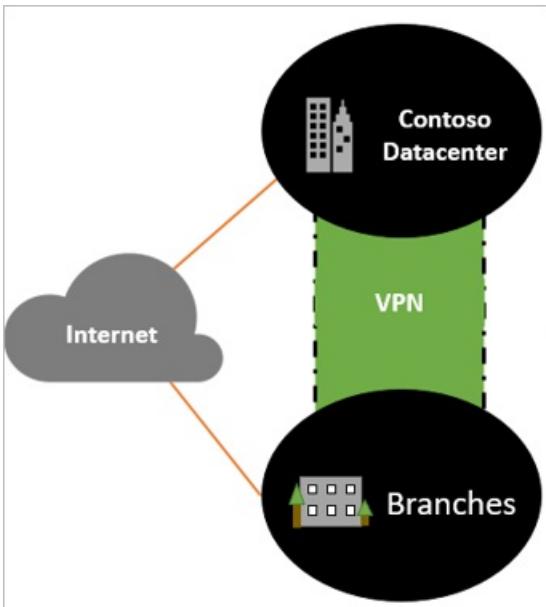
With the regional design in place, Contoso is ready to consider a network strategy. It needs to think about how the on-premises datacenter and Azure connect and communicate with each other, and how to design the network infrastructure in Azure. Specifically, Contoso needs to:

- **Plan hybrid network connectivity.** Figure out how it's going to connect networks across on-premises and Azure.
- **Design an Azure network infrastructure.** Decide how it will deploy networks over regions. How will networks communicate within the same region and across regions?
- **Design and set up Azure networks.** Set up Azure networks and subnets, and decide what will reside in them.

#### Plan hybrid network connectivity

Contoso considered [several architectures for hybrid networking](#) between Azure and the on-premises datacenter. For more information, see [Choose a solution for connecting an on-premises network to Azure](#).

As a reminder, the Contoso on-premises network infrastructure currently consists of the datacenter in New York, and local branches in the eastern half of the United States. All locations have a business-class connection to the internet. Each of the branches is then connected to the datacenter via an IPsec VPN tunnel over the internet.

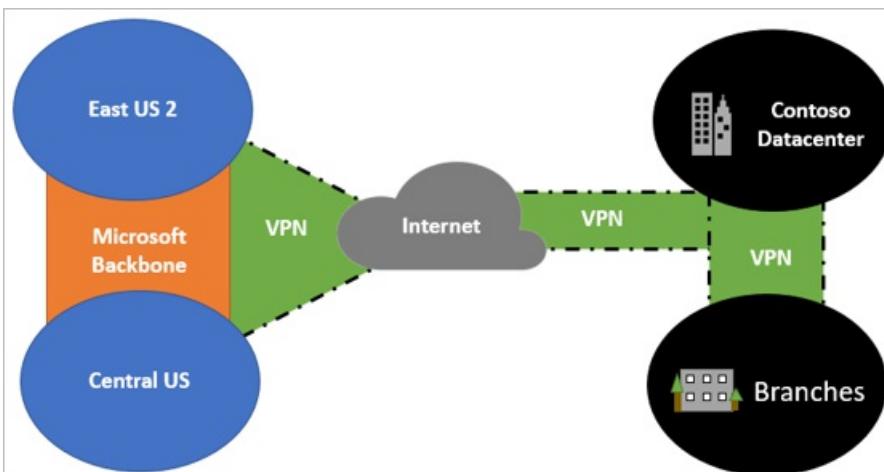


*Figure 15: The Contoso network.*

Here's how Contoso decided to implement hybrid connectivity:

1. Set up a new Site-to-Site VPN connection between the Contoso datacenter in New York and the two Azure regions, **East US 2** and **Central US**.
2. Branch office traffic bound for virtual networks in Azure will route through the main Contoso datacenter.
3. As Contoso scales up Azure deployment, it will establish an Azure ExpressRoute connection between the datacenter and the Azure regions. When this happens, Contoso will retain the VPN Site-to-Site connection for failover purposes only.
  - Learn more about [choosing between a VPN and ExpressRoute hybrid solution](#).
  - Verify [ExpressRoute locations and support](#).

**VPN only:**



*Figure 16: The Contoso VPN.*

**VPN and ExpressRoute:**

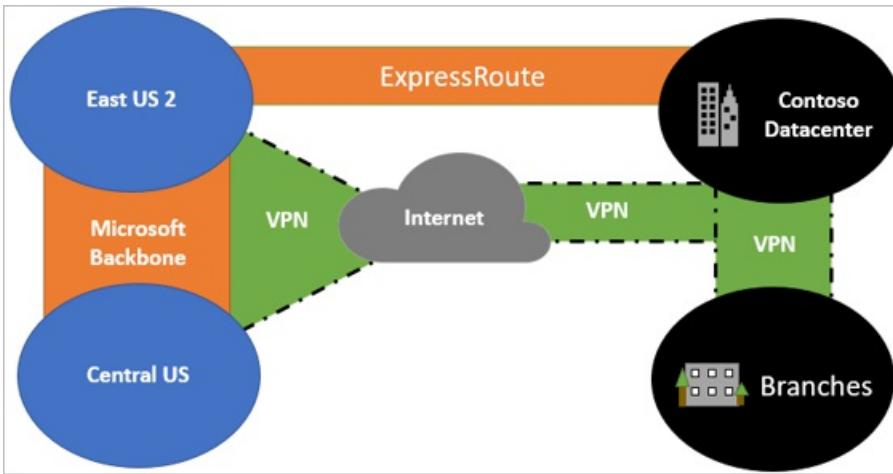


Figure 17: Contoso VPN and ExpressRoute.

### Design the Azure network infrastructure

Contoso's network configuration must make the hybrid deployment secure and scalable. Contoso is taking a long-term approach to this, designing virtual networks to be resilient and enterprise ready. For more information, see [Plan virtual networks](#).

To connect the two regions, Contoso will implement a hub-to-hub network model. Within each region, Contoso will use a hub-and-spoke model. To connect networks and hubs, Contoso will use Azure network peering.

#### Network peering

[Virtual network peering](#) in Azure connects virtual networks and hubs. Global peering allows connections between virtual network or hubs in different regions. Local peering connects virtual networks in the same region.

Virtual network peering provides several advantages:

- Network traffic between peered virtual networks is private.
- Traffic between the virtual networks is kept on the Microsoft backbone network. No public internet, gateways, or encryption is required in the communication between the virtual networks.
- Peering provides a default, low-latency, high-bandwidth connection between resources in different virtual networks.

#### Hub-to-hub model across regions

Contoso will deploy a hub in each region. A hub is a virtual network in Azure that acts as a central point of connectivity to your on-premises network. The hub virtual networks will connect to each other via global virtual network peering, which connects virtual networks across Azure regions. The hub in each region is peered to its partner hub in the other region. The hub is peered to every network in its region, and it can connect to all network resources.

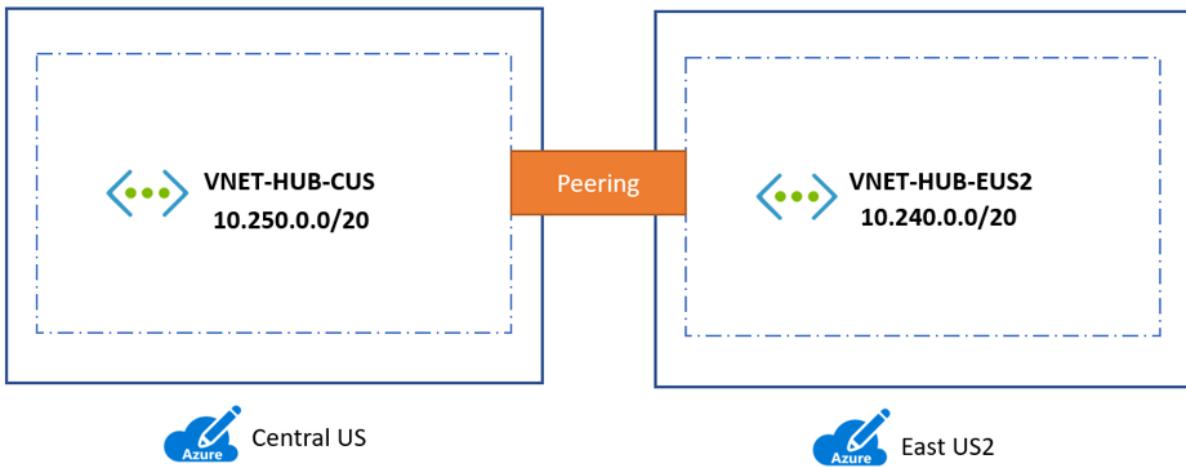


Figure 18: Global peering.

#### **Hub-and-spoke model within a region**

Within each region, Contoso will deploy virtual networks for different purposes as spoke networks from the region hub. Virtual networks within a region use peering to connect to their hub and to each other.

#### **Design the hub network**

Within the hub-and-spoke model, Contoso needed to think about how traffic from the on-premises datacenter and from the internet would be routed. Here's how Contoso decided to handle routing for both the **East US 2** and **Central US** hubs:

- Contoso is designing a network that allows traffic from the internet and from the corporate network by using a VPN to Azure.
- The network architecture has two boundaries, an untrusted front-end perimeter zone and a back-end trusted zone.
- A firewall will have a network adapter in each zone, controlling access to trusted zones.
- From the internet:
  - Internet traffic will hit a load-balanced public IP address on the perimeter network.
  - This traffic is routed through the firewall and subject to firewall rules.
  - After network access controls are implemented, traffic will be forwarded to the appropriate location in the trusted zone.
  - Outbound traffic from the virtual network will be routed to the internet through user-defined routes. The traffic is forced through the firewall and inspected in line with Contoso policies.
- From the Contoso datacenter:
  - Incoming traffic over Site-to-Site VPN or ExpressRoute hits the public IP address of the Azure VPN gateway.
  - Traffic is routed through the firewall and subject to firewall rules.
  - After the application of firewall rules, traffic is forwarded to an internal load balancer (Standard SKU) on the trusted internal zone subnet.
  - Outbound traffic from the trusted subnet to the on-premises datacenter over the VPN is routed through the firewall. Rules are applied before traffic goes over the Site-to-Site VPN connection.

#### **Design and set up Azure networks**

With a network and routing topology in place, Contoso is ready to set up Azure networks and subnets:

- Contoso will implement a class-A private network in Azure (**10.0.0.0/8**). This works because of on-premises; it currently has a class-B private address space (**172.160.0.0/16**). Contoso can be sure there won't be any overlap between address ranges.
- Contoso will deploy virtual networks in both the primary and secondary regions.
- Contoso will use a naming convention that includes the prefix **VNET** and the region abbreviation **EUS2**.

or **cus**. Using this standard, the hub networks will be named **VNET-HUB-EUS2** in the **East US 2** region and **VNET-HUB-CUS** in the **central US** region.

#### Virtual networks in **East US 2**

**East US 2** is the primary region that Contoso will use to deploy resources and services. Here's how Contoso will design networks in that region:

- **Hub:** The hub virtual network in **East us 2** is considered Contoso's primary connectivity to the on-premises datacenter.
- **Virtual networks:** The spoke virtual networks in **East us 2** can be used to isolate workloads if necessary. In addition to the hub virtual network, Contoso will have two spoke virtual networks in **East US 2**:
  - **VNET-DEV-EUS2**. This virtual network will provide the dev/test team with a fully functional network for dev projects. It will act as a production pilot area, and will rely on the production infrastructure to function.
  - **VNET-PROD-EUS2**. Azure IaaS production components will be located in this network. Each virtual network will have its own unique address space without overlap. Contoso intends to configure routing without requiring network address translation (NAT).
- **Subnets:** There will be a subnet in each network for each application tier. Each subnet in the production network will have a matching subnet in the development virtual network. The production network has a subnet for domain controllers.

The following table summarizes virtual networks in **East US 2**.

VIRTUAL NETWORK	RANGE	PEER
<b>VNET-HUB-EUS2</b>	<b>10.240.0.0/20</b>	<b>VNET-HUB-CUS2</b> , <b>VNET-DEV-EUS2</b> , <b>VNET-PROD-EUS2</b>
<b>VNET-DEV-EUS2</b>	<b>10.245.16.0/20</b>	<b>VNET-HUB-EUS2</b>
<b>VNET-PROD-EUS2</b>	<b>10.245.32.0/20</b>	<b>VNET-HUB-EUS2</b> , <b>VNET-PROD-CUS</b>

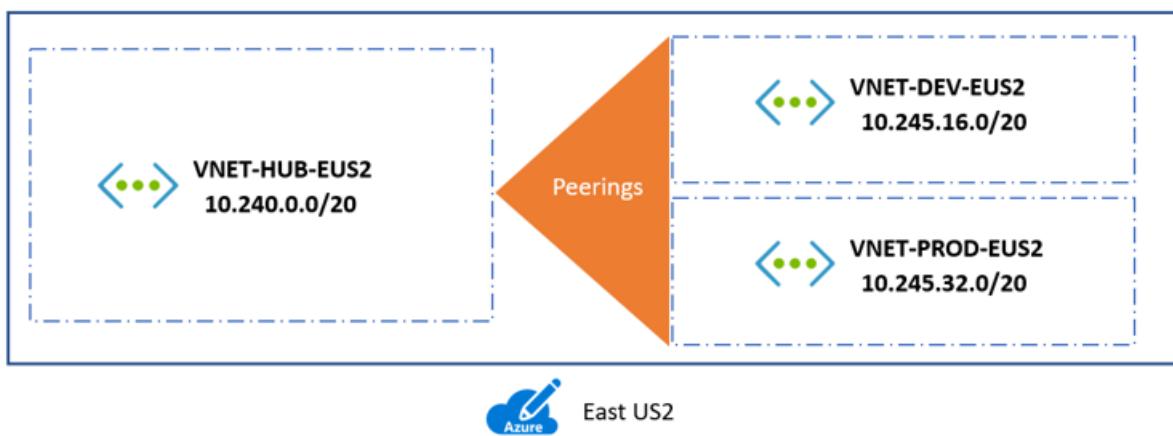


Figure 19: A hub-and-spoke model.

**Subnets in the **East US 2 Hub** network (**VNET-HUB-EUS2**)**

SUBNET/ZONE	CIDR	USABLE IP ADDRESSES
IB-UntrustZone	10.240.0.0/24	251
IB-TrustZone	10.240.1.0/24	251
OB-UntrustZone	10.240.2.0/24	251
OB-TrustZone	10.240.3.0/24	251
GatewaySubnet	10.240.10.0/24	251

#### Subnets in the `East US 2` development network (`VNET-DEV-EUS2`)

The development team uses the development virtual network as a production pilot area. It has three subnets.

SUBNET	CIDR	ADDRESSES	IN SUBNET
DEV-FE-EUS2	10.245.16.0/22	1019	Front ends/web-tier VMs
DEV-APP-EUS2	10.245.20.0/22	1019	Application-tier VMs
DEV-DB-EUS2	10.245.24.0/23	507	Database VMs

#### Subnets in the `East US 2` production network (`VNET-PROD-EUS2`)

Azure IaaS components are located in the production network. Each application tier has its own subnet. Subnets match those in the development network, with the addition of a subnet for domain controllers.

SUBNET	CIDR	ADDRESSES	IN SUBNET
PROD-FE-EUS2	10.245.32.0/22	1019	Front ends/web-tier VMs
PROD-APP-EUS2	10.245.36.0/22	1019	Application-tier VMs
PROD-DB-EUS2	10.245.40.0/23	507	Database VMs
PROD-DC-EUS2	10.245.42.0/24	251	Domain controller VMs

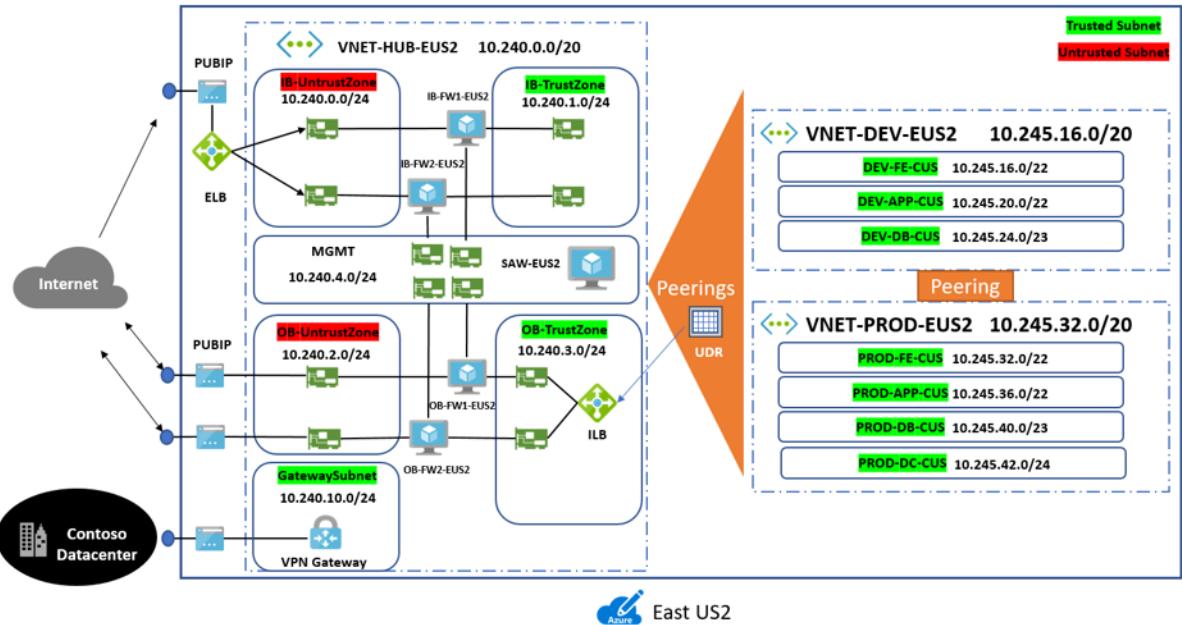


Figure 20: Hub network architecture.

#### Virtual networks in **Central US** (secondary region)

**Central US** is Contoso's secondary region. Here's how Contoso will architect networks within it:

- **Hub:** The hub virtual network in **Central US** is considered the secondary point of connectivity to the on-premises datacenter. The spoke virtual networks in **Central US** can be used to isolate workloads if necessary, managed separately from other spokes.
- **Virtual networks:** Contoso will have two virtual networks in **Central US** :
  - **VNET-PROD-CUS** : This is a production network and can be thought of as a secondary hub.
  - **VNET-ASR-CUS** : This virtual network will act as a location in which VMs are created after failover from on-premises or as a location for Azure VMs failed over from the primary to the secondary region. This network is similar to the production networks but without any domain controllers on it.

Each virtual network in the region will have its own address space without overlap. Contoso will configure routing without NAT.

- **Subnets:** The subnets will be designed in a similar way to those in **East US 2**.

The following table summarizes virtual networks in **Central US**.

VIRTUAL NETWORK	RANGE	PEER
VNET-HUB-CUS	10.250.0.0/20	VNET-HUB-EUS2 , VNET-ASR-CUS , VNET-PROD-CUS
VNET-ASR-CUS	10.255.16.0/20	VNET-HUB-CUS , VNET-PROD-CUS
VNET-PROD-CUS	10.255.32.0/20	VNET-HUB-CUS , VNET-ASR-CUS , VNET-PROD-EUS2

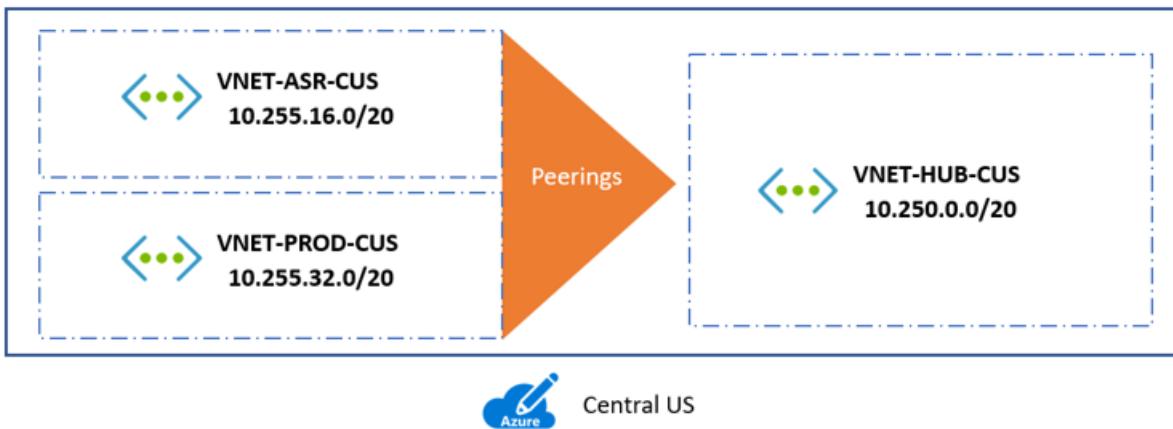


Figure 21: A hub-and-spoke model in a paired region.

#### Subnets in the Central US hub network ( VNET-HUB-CUS )

SUBNET	CIDR	USABLE IP ADDRESSES
IB-UntrustZone	10.250.0.0/24	251
IB-TrustZone	10.250.1.0/24	251
OB-UntrustZone	10.250.2.0/24	251
OB-TrustZone	10.250.3.0/24	251
GatewaySubnet	10.250.2.0/24	251

#### Subnets in the Central US production network ( VNET-PROD-CUS )

In parallel with the production network in the primary region ( East US 2 ), there's a production network in the secondary region ( Central US ).

SUBNET	CIDR	ADDRESSES	IN SUBNET
PROD-FE-CUS	10.255.32.0/22	1019	Front ends/web-tier VMs
PROD-APP-CUS	10.255.36.0/22	1019	Application-tier VMs
PROD-DB-CUS	10.255.40.0/23	507	Database VMs
PROD-DC-CUS	10.255.42.0/24	251	Domain controller VMs

#### Subnets in the Central US failover/recovery network ( VNET-ASR-CUS )

The VNET-ASR-CUS network is used for failover between regions. Site Recovery will be used to replicate and fail over Azure VMs between the regions. It also functions as a Contoso datacenter to the Azure network for protected workloads that remain on-premises but fail over to Azure for disaster recovery.

VNET-ASR-CUS is the same basic subnet as the production virtual network in East US 2 but without the need for a domain controller subnet.

SUBNET	CIDR	ADDRESSES	IN SUBNET
ASR-FE-CUS	10.255.16.0/22	1019	Front ends/web-tier VMs

SUBNET	CIDR	ADDRESSES	IN SUBNET
ASR-APP-CUS	10.255.20.0/22	1019	Application-tier VMs
ASR-DB-CUS	10.255.24.0/23	507	Database VMs

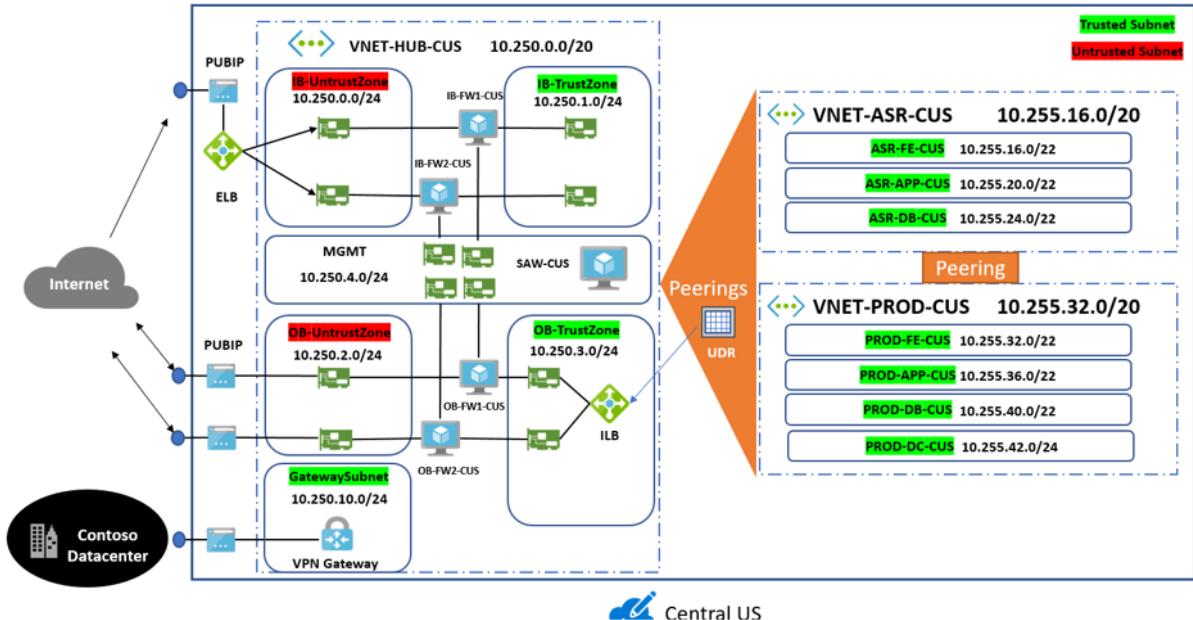


Figure 22: Hub network architecture.

#### Configure peered connections

The hub in each region will be peered to the hub in the other region and to all virtual networks within the hub region. This configuration allows for hubs to communicate and to view all virtual networks within a region. Note that peering creates a two-sided connection. One is from the initiating peer on the first virtual network, and the other is on the second virtual network.

In a hybrid deployment, traffic that passes between peers needs to be visible from the VPN connection between the on-premises datacenter and Azure. To enable this, Contoso must use specific settings on peered connections. For any connections from spoke virtual networks through the hub to the on-premises datacenter, Contoso needs to allow traffic to be forwarded and to cross the VPN gateways.

#### Domain controller

For the domain controllers in the VNET-PROD-EUS2 network, Contoso wants traffic to flow both between the EUS2 hub/production network and over the VPN connection to on-premises. To do this, Contoso admins must allow the following:

1. Allow forwarded traffic and Allow gateway transit configurations on the peered connection.

In our example, this would be the connection from VNET-HUB-EUS2 to VNET-PROD-EUS2.



Figure 23: A peered connection.

2. Allow **forwarded traffic** and **Use remote gateways** on the other side of the peering, on the connection from **VNET-PROD-EUS2** to **VNET-HUB-EUS2**.

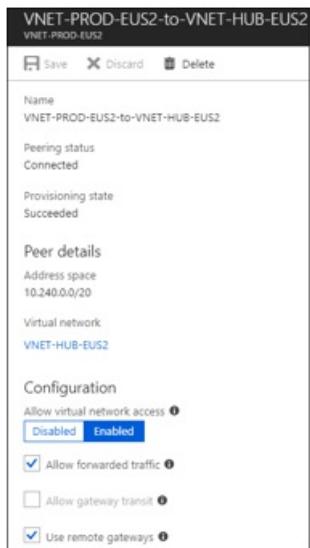


Figure 24: A peered connection.

3. On-premises, they set up a static route that directs the local traffic to route across the VPN tunnel to the virtual network. The configuration is completed on the gateway that provides the VPN tunnel from Contoso to Azure. They use routing and remote access service (RRAS) for the static route.

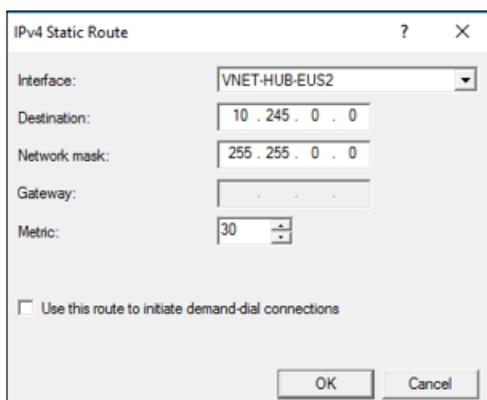


Figure 25: A peered connection.

#### Production networks

A spoked peer network can't see a spoked peer network in another region via a hub. For Contoso's production networks in both regions to see each other, Contoso admins need to create a direct peered connection for **VNET-PROD-EUS2** and **VNET-PROD-CUS**.

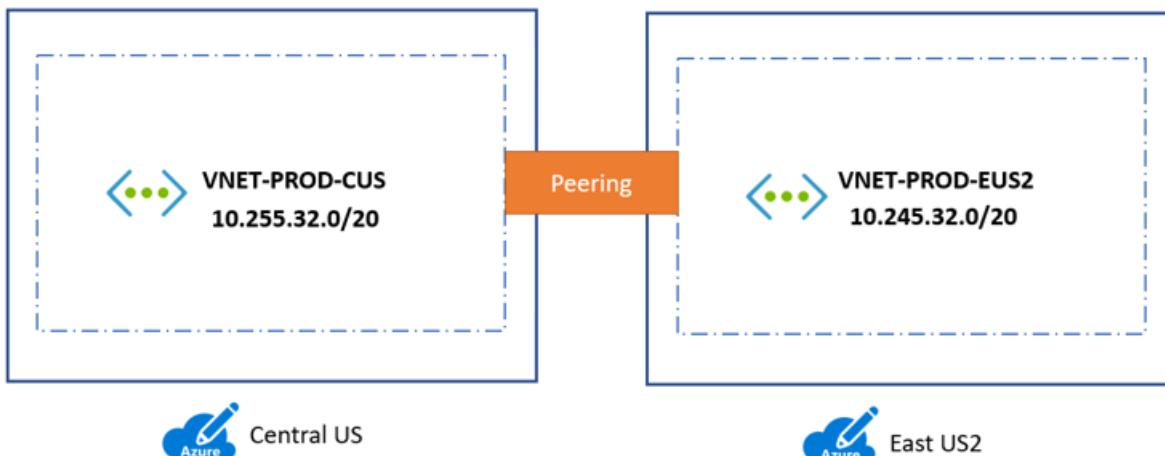


Figure 26: Creating a direct peered connection.

#### Set up DNS

When you deploy resources in virtual networks, you have a couple of choices for domain name resolution. You can use name resolution provided by Azure or provide DNS servers for resolution. The type of name resolution that you use depends on how your resources need to communicate with each other. Get [more information](#) about the Azure DNS service.

Contoso admins have decided that the Azure DNS service isn't a good choice in the hybrid environment. Instead, they'll use the on-premises DNS servers. Here are the details:

- Because this is a hybrid network, all VMs on-premises and in Azure need to be able to resolve names to function properly. This means that custom DNS settings must be applied to all the virtual networks.
- Contoso currently has domain controllers (DCs) deployed in the Contoso datacenter and at the branch offices. The primary DNS servers are **contosodc1** ( 172.16.0.10 ) and **contosodc2** ( 172.16.0.1 ).
- After the virtual networks are deployed, the on-premises domain controllers are configured as DNS servers in the networks.
- If an optional custom DNS is specified for the virtual network, the virtual IP address **168.63.129.16** for the recursive resolvers in Azure must be added to the list. To do this, Contoso configures DNS server settings on each virtual network. For example, the custom DNS settings for the **VNET-HUB-EUS2** network would be as follows:

Figure 27: A custom DNS.

In addition to the on-premises domain controllers, Contoso will implement four domain controllers to support the Azure networks (two for each region):

REGION	DC	VIRTUAL NETWORK	SUBNET	IP ADDRESS
East US 2	contosodc3	VNET-PROD-EUS2	PROD-DC-EUS2	10.245.42.4
East US 2	contosodc4	VNET-PROD-EUS2	PROD-DC-EUS2	10.245.42.5
Central US	contosodc5	VNET-PROD-CUS	PROD-DC-CUS	10.255.42.4
Central US	contosodc6	VNET-PROD-CUS	PROD-DC-CUS	10.255.42.4

After deploying the on-premises domain controllers, Contoso needs to update the DNS settings on networks on either region to include the new domain controllers in the DNS server list.

#### Set up domain controllers in Azure

After updating network settings, Contoso admins are ready to build out the domain controllers in Azure.

1. In the Azure portal, they deploy a new Windows Server VM to the appropriate virtual network.
2. They [create availability sets](#) in each location for the VM. Availability sets ensure that the Azure fabric separates the VMs into different infrastructures in the Azure region. Availability sets also allow Contoso to be eligible for the 99.95 percent service-level agreement (SLA) for VMs in Azure.

Figure 28: An availability set.

3. After the VM is deployed, they open the network interface for the VM. They set the private IP address

to static and specify a valid address.

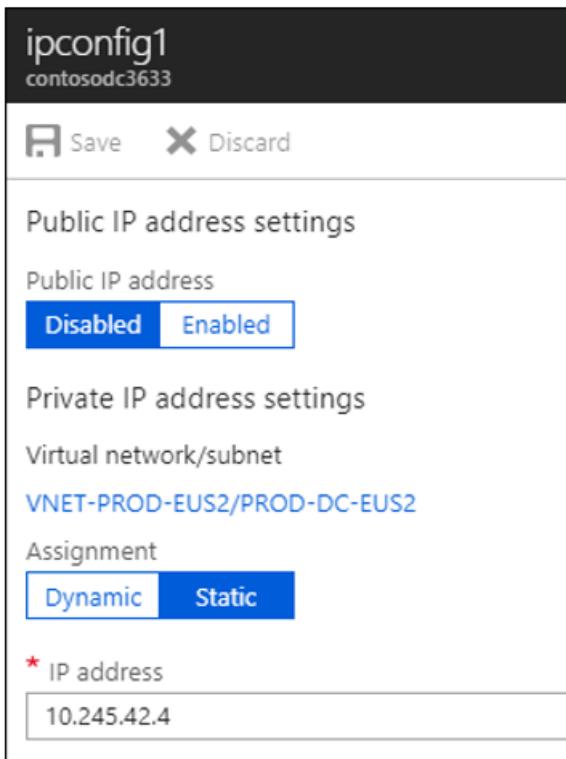


Figure 29: A VM NIC.

4. They attach a new data disk to the VM. This disk contains the Active Directory database and the SYSVOL share.

The size of the disk will determine the number of IOPS that it supports. Over time, the disk size might need to increase as the environment grows.

**NOTE**

The disk shouldn't be set to read/write for host caching. Active Directory databases don't support this.

<input type="checkbox"/>	<b>CONTOSODC3</b>	Virtual machine
<input type="checkbox"/>	<b>CONTOSODC3_OsDisk_...</b>	Disk
<input type="checkbox"/>	<b>CONTOSODC3-Data-Disk</b>	Disk

Figure 30: An Active Directory disk.

5. After the disk is added, they connect to the VM over Remote Desktop Services and open Server Manager.
6. In **File and Storage Services**, they run the New Volume Wizard. They ensure that the drive is assigned the letter F or above on the local VM.

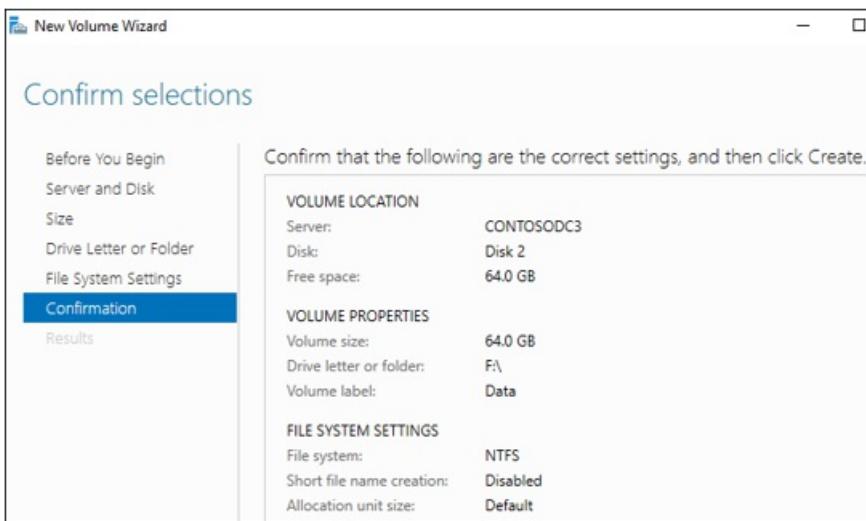


Figure 31: New Volume Wizard.

7. In Server Manager, they add the **Active Directory Domain Services** role. Then, they configure the VM as a domain controller.

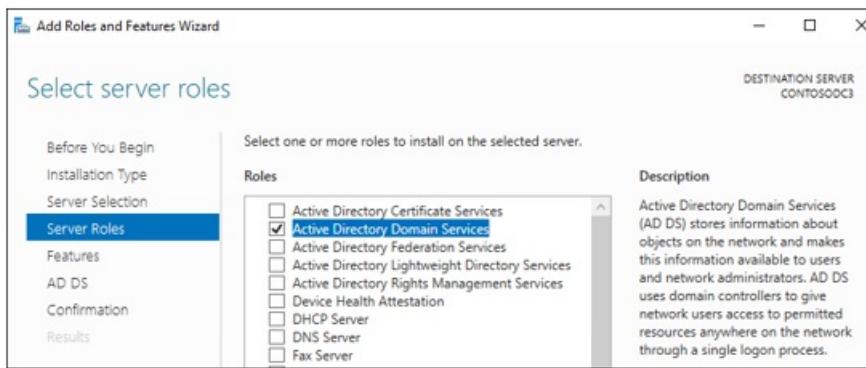


Figure 32: Adding the server role.

8. After the VM is configured as a DC and restarted, they open DNS manager and configure the Azure DNS resolver as a forwarder. This allows the DC to forward DNS queries it can't resolve in the Azure DNS.

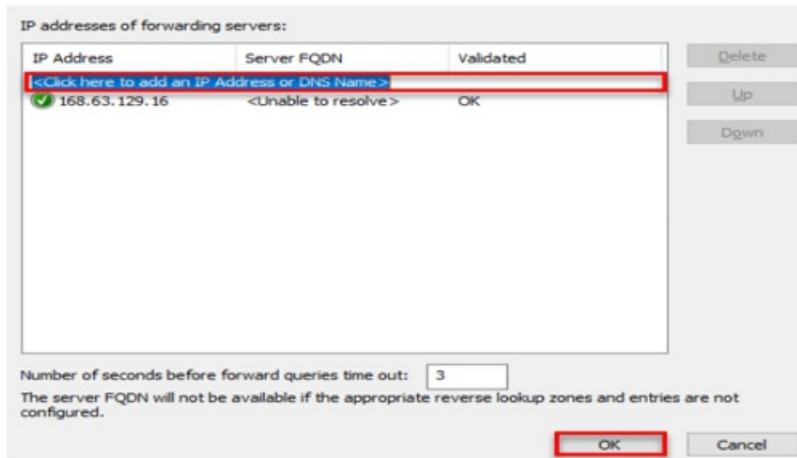


Figure 33: Configuring the Azure DNS resolver.

9. They update the custom DNS settings for each virtual network with the appropriate domain controller for the virtual network region. They include on-premises DCs in the list.

## Set up Active Directory

Active Directory is a critical service for a network and must be configured correctly. Contoso admins will build Active Directory sites for the Contoso datacenter and for the **East US 2** and **Central US** regions.

1. They create two new sites (**AZURE-EUS2** and **AZURE-CUS**) along with the datacenter site (**contoso-datacenter**).
2. After creating the sites, they create subnets in the sites, to match the virtual networks and datacenter.

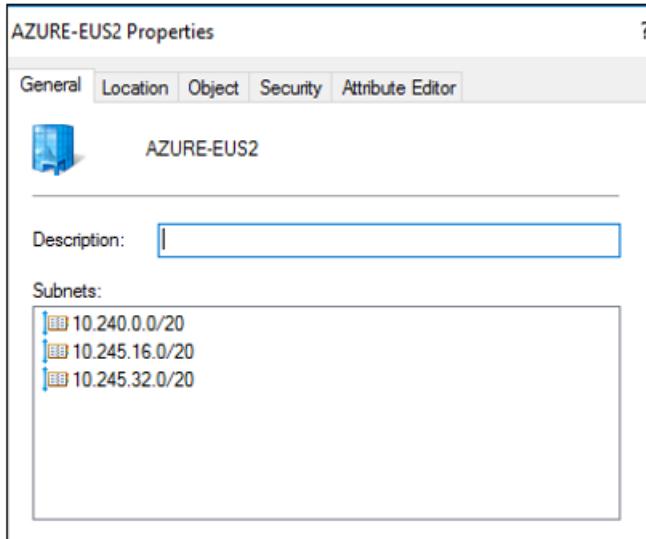


Figure 34: Datacenter subnets.

3. They create two site links to connect everything. The domain controllers should then be moved to their location.

Name	Type
ContosoDatacenter-To-Azure-CUS	Site Link
ContosoDatacenter-To-Azure-EUS2	Site Link

Figure 35: Datacenter links.

4. They confirm that the Active Directory replication topology is in place.

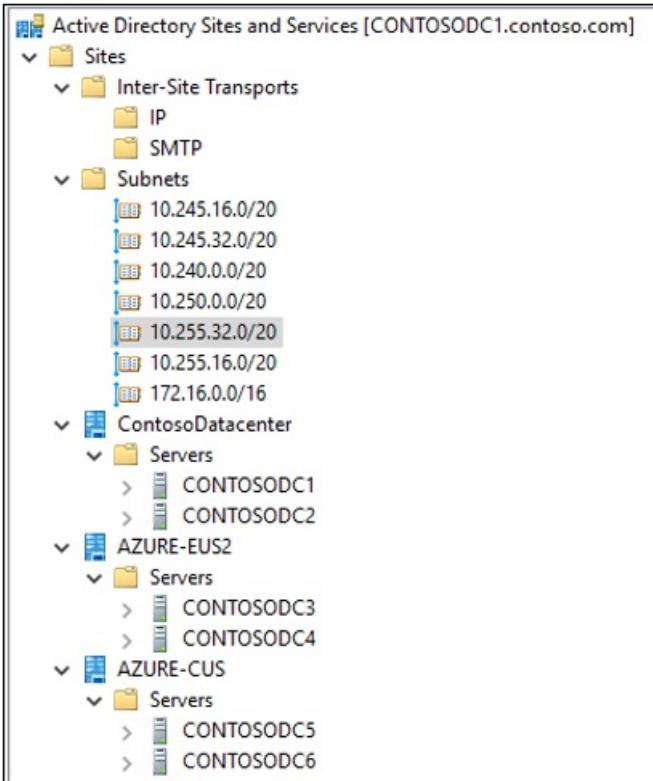


Figure 36: Datacenter replication.

With everything complete, a list of the domain controllers and sites is shown in the on-premises Active Directory Administrative Center.

Name	Site	Type	Domain Controller...	Description
CONTOSODC1	ContosoDatacenter	Domain Controller	Global Catalog	
CONTOSODC2	ContosoDatacenter	Domain Controller	Global Catalog	
CONTOSODC3	AZURE-EUS2	Domain Controller	Global Catalog	
CONTOSODC4	AZURE-EUS2	Domain Controller	Global Catalog	
CONTOSODC5	AZURE-CUS	Domain Controller	Global Catalog	
CONTOSODC6	AZURE-CUS	Domain Controller	Global Catalog	

Figure 37: The Active Directory Administrative Center.

## Step 5: Plan for governance

Azure provides a range of governance controls across services and the Azure platform. For more information, see the [Azure governance options](#).

As it configures identity and access control, Contoso has already begun to put some aspects of governance and security in place. Broadly, it needs to consider three areas:

- **Policy:** Azure Policy applies and enforces rules and effects over your resources, so the resources comply with corporate requirements and SLAs.
- **Locks:** Azure allows you to lock subscriptions, resource groups, and other resources so that they can be modified only by those with permissions.
- **Tags:** Resources can be controlled, audited, and managed with tags. Tags attach metadata to resources, providing information about resources or owners.

## Set up policies

The Azure Policy service evaluates your resources by scanning for those not compliant with policy definitions. For example, you might have a policy that only allows certain types of VMs or requires resources to have a specific tag.

Policies specify a policy definition, and a policy assignment specifies the scope in which a policy should be applied. The scope can range from a management group to a resource group. Learn how to [create and manage policies](#).

Contoso wants to begin two policies. It wants a policy to ensure that resources can be deployed in the `East US 2` and `Central US` regions only. It also wants a policy to limit VM SKUs to approved SKUs only. The intention is to ensure that expensive VM SKUs aren't used.

### Limit resources to regions

Contoso uses the built-in policy definition **Allowed locations** to limit resource regions.

1. In the Azure portal, select **All services**, and search for **Policy**.
2. Select **Assignments > Assign policy**.
3. In the policy list, select **Allowed locations**.
4. Set **Scope** to the name of the Azure subscription, and select the two regions in the allowlist.

The screenshot shows the Azure Policy assignments interface. At the top, there are three buttons: 'Assign Policy', 'Assign Initiative', and 'Refresh'. Below these are filters for 'Scope' (a dropdown menu), 'Type' (set to 'All types'), 'Search' (an input field), and a 'Filter' button. Below the filters, there are three summary metrics: 'Total Assignments' (1), 'Initiative Assignments' (0), and 'Policy Assignments' (1). The main table below has columns for 'NAME', 'SCOPE', and 'TYPE'. A single row is visible, labeled 'Allowed locations' under 'NAME', with 'Policy' under 'TYPE'. The 'SCOPE' column shows a blurred value.

Figure 38: Allowed locations defined via policy.

5. By default, the policy is set with **Deny**. This setting means that if someone starts a deployment in the subscription that isn't in either the `East US 2` or `Central US` region, the deployment will fail. Here's what happens if someone in the Contoso subscription tries to set up a deployment in `West US`.

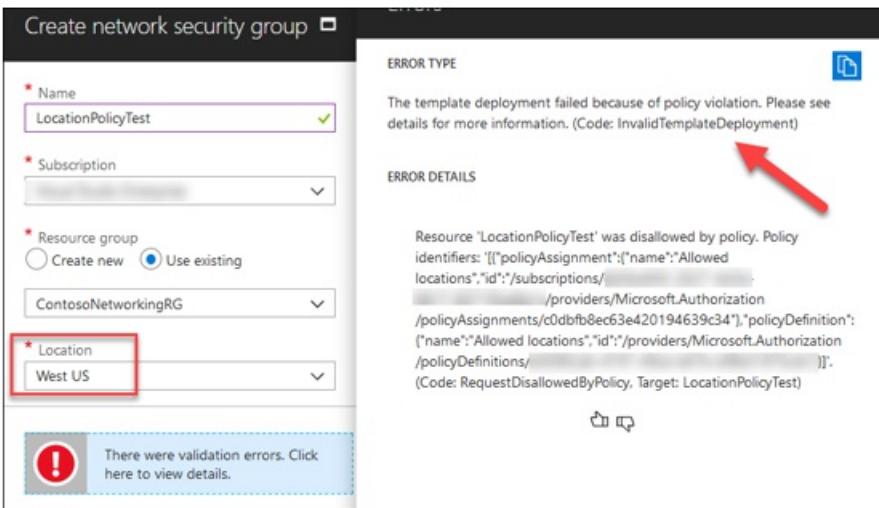


Figure 39: A failed policy.

#### Allow specific VM SKUs

Contoso will use the built-in policy definition `Allow virtual machine SKUs` to limit the types of VMs that can be created in the subscription.

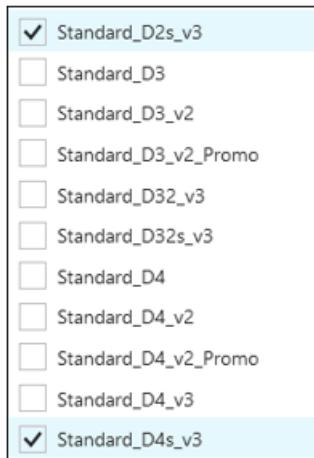


Figure 40: A policy SKU.

#### Check policy compliance

Policies go into effect immediately, and Contoso can check resources for compliance. In the Azure portal, select the **Compliance** link. The compliance dashboard appears. You can drill down for more details.

The screenshot shows the 'Policy - Compliance' blade in the Azure portal. The left sidebar has links for Overview, Getting started, and Compliance (which is selected). The main area has sections for Non-compliant initiatives (0), Non-compliant policies (1), and Non-compliant resources (13). Below these are tables for 'NAME', 'SCOPE', 'COMPLIANCE', 'TYPE', and 'NON-COMPLIANT'. The first row shows 'Allowed locations' with Visual Studio Enterprise scope, non-compliant status, and a policy type. The second row shows 'Allowed virtual machine SKUs' with Visual Studio Enterprise scope, compliant status, and a policy type.

NAME	SCOPE	COMPLIANCE	TYPE	NON-COMPLIANT
Allowed locations	Visual Studio Enterprise	Non-compliant	Policy	1
Allowed virtual machine SKUs	Visual Studio Enterprise	Compliant	Policy	0

Figure 41: Policy compliance.

## Set up locks

Contoso has long been using the ITIL framework for the management of its systems. One of the most important aspects of the framework is change control, and Contoso wants to make sure that change control is implemented in the Azure deployment.

Contoso will [lock resources](#). Any production or failover component must be in a resource group that has a read-only lock. This means that to modify or delete production items, authorized users must remove the lock. Nonproduction resource groups will have `CanNotDelete` locks. This means that authorized users can read or modify a resource but can't delete it.

## Set up tagging

To track resources as they're added, it will be increasingly important for Contoso to associate resources with an appropriate department, customer, and environment. In addition to providing information about resources and owners, tags will enable Contoso to aggregate and group resources and to use that data for chargeback purposes.

Contoso needs to visualize its Azure assets in a way that makes sense for the business, such as by role or department. Note that resources don't need to reside in the same resource group to share a tag. Contoso will create a tag taxonomy so that everyone uses the same tags.

TAG NAME	VALUE
<code>CostCenter</code>	12345: It must be a valid cost center from SAP.
<code>BusinessUnit</code>	Name of the business unit (from SAP). Matches <code>CostCenter</code> .
<code>ApplicationTeam</code>	Email alias of the team that owns support for the application.
<code>CatalogName</code>	Name of the application or <code>SharedServices</code> , according to the service catalog that the resource supports.
<code>ServiceManager</code>	Email alias of the ITIL Service Manager for the resource.
<code>COBPriority</code>	Priority set by the business for BCDR. Values of 1-5.
<code>ENV</code>	<code>DEV</code> , <code>STG</code> , and <code>PROD</code> are the allowed values, representing development, staging, and production.

For example:

CostCenter : 12345
BusinessUnit : IT
ApplicationTeam : IT-Networking@contoso.com
CatalogName : SharedServices
COBPriority : 1
ENV : PROD
ServiceManager : chad@contoso.com

Figure 42: Azure tags.

After creating the tag, Contoso will go back and create new policy definitions and assignments to enforce the use of the required tags across the organization.

## Step 6: Consider security

Security is crucial in the cloud, and Azure provides a wide array of security tools and capabilities. These help you to create secure solutions on the secure Azure platform. See [Trust your cloud](#) to learn more about Azure security.

There are a few aspects for Contoso to consider:

- [Azure Security Center](#) provides unified security management and Azure Advanced Threat Protection across hybrid cloud workloads. Use it to apply security policies across your workloads, limit your exposure to threats, and detect and respond to attacks.
- A [network security group \(NSG\)](#) filters network traffic based on a list of security rules that allow or deny network traffic to resources connected to virtual networks in Azure.
- [Azure Disk Encryption](#) is a capability that helps you encrypt your Windows and Linux IaaS VM disks.

### Work with the Azure Security Center

Contoso is looking for a quick view into the security posture of its new hybrid cloud, and specifically, its Azure workloads. As a result, Contoso has decided to implement Azure Security Center starting with the following features:

- Centralized policy management
- Continuous assessment
- Actionable recommendations

#### Centralize policy management

With centralized policy management, Contoso will ensure compliance with security requirements by centrally managing security policies across the entire environment. It can simply and quickly implement a policy that applies to all of its Azure resources.

The screenshot shows a user interface for managing security policies. On the left, there's a sidebar titled 'POLICY COMPONENTS' with icons for Data Collection, Security policy (which is selected and highlighted in blue), Email notifications, and Pricing tier. At the top right are 'Save' and 'Cancel' buttons. The main area is titled 'Show recommendations for' and lists ten policy components with 'On' or 'Off' status indicators and 'UPGRADE' buttons:

Policy Component	Status	Action
System updates	On	Off
Security configurations	On	Off
Endpoint protection	On	Off
Disk encryption	On	Off
Network security groups	On	Off
Web application firewall	On	Off
Next generation firewall	On	Off
Vulnerability Assessment	On	Off
Storage Encryption	On	Off
JIT Network Access	On	Off
Adaptive Application Controls	On	Off
SQL auditing & Threat detection	On	Off
SQL Encryption	On	Off

Figure 43: A security policy.

#### Assess security

Contoso will take advantage of the continuous security assessment that monitors the security of machines, networks, storage, data, and applications to discover potential security issues.

Security Center analyzes the security state of the Contoso compute, infrastructure, and data resources. It also analyzes the security state of Azure apps and services. Continuous assessment helps the Contoso operations team to discover potential security issues, such as systems with missing security updates or exposed network ports.

Contoso wants to make sure all of the VMs are protected. Security Center helps with this. It verifies VM health, and it makes prioritized and actionable recommendations to remediate security vulnerabilities before they're exploited.

## Endpoint Protection not installed on Azure VMs



VIRTUAL MACHINE	STATE	SEVERITY	...
<input checked="" type="checkbox"/> CONTOSODC3	Open	! High	...
<input checked="" type="checkbox"/> CONTOSODC4	Open	! High	...
<input checked="" type="checkbox"/> CONTOSODC5	Open	! High	...
<input checked="" type="checkbox"/> CONTOSODC6	Open	! High	...

Figure 44: Monitoring.

### Work with NSGs

Contoso can limit network traffic to resources in a virtual network by using network security groups.

A network security group contains a list of security rules that allow or deny inbound or outbound network traffic based on source or destination IP address, port, and protocol. When applied to a subnet, rules are applied to all resources in the subnet. In addition to network interfaces, this includes instances of Azure services deployed in the subnet.

Application security groups (ASGs) enable you to configure network security as a natural extension of an application structure. You can then group VMs and define network security policies based on those groups.

Contoso can use ASGs to reuse the security policy at scale without manual maintenance of explicit IP addresses. The platform handles the complexity of explicit IP addresses and multiple rule sets, so the organization can focus on business logic. Contoso can specify an ASG as the source and destination in a security rule. After a security policy is defined, Contoso can create VMs and assign the VM NICs to a group.

Contoso will implement a mix of NSGs and ASGs. Contoso is concerned about NSG management. It's also worried about the overuse of NSGs and the added complexity for operations staff. Here's what Contoso will do:

- All traffic into and out of all subnets (north/south) will be subject to an NSG rule, except for the gateway subnets in the hub networks.
- Any firewalls or domain controllers will be protected by both subnet NSGs and NIC NSGs.
- All production applications will have ASGs applied.

Contoso has built a model of how this security configuration will look for its applications.

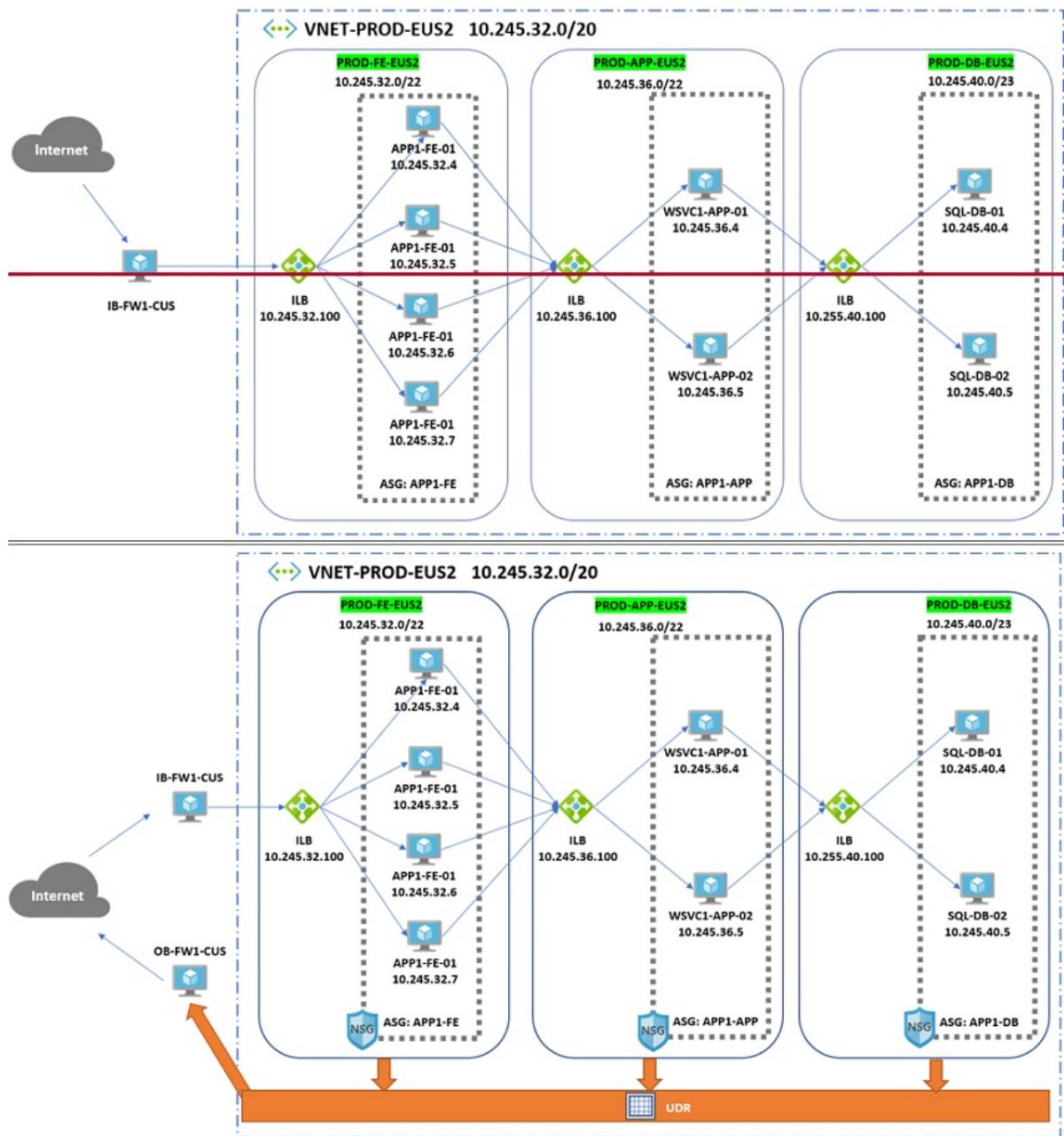


Figure 45: Security model.

The NSGs associated with the ASGs will be configured with least privilege to ensure that only allowed packets can flow from one part of the network to its destination.

ACTION	NAME	SOURCE	TARGET	PORT
Allow	AllowInternetToFE	VNET-HUB-EU2 / IB-TrustZone	APP1-FE	80, 443
Allow	AllowWebToApp	APP1-FE	APP1-APP	80, 443
Allow	AllowAppToDB	APP1-APP	APP1-DB	1433
Deny	DenyAllInbound	Any	Any	Any

### Encrypt data

Azure Disk Encryption integrates with Azure Key Vault to help control and manage the disk-encryption keys and secrets for a subscription. It ensures that all data on VM disks is encrypted at rest in Azure Storage.

Contoso has determined that specific VMs require encryption. Contoso will apply encryption to VMs with customer, confidential, or personal data.

## Conclusion

In this article, Contoso set up an Azure infrastructure and policy for Azure subscription, hybrid identify, disaster recovery, network, governance, and security.

Not every step taken here is required for a cloud migration. In this case, Contoso planned a network infrastructure that can handle all types of migrations while being secure, resilient, and scalable.

## Next steps

After setting up its Azure infrastructure, Contoso is ready to begin migrating workloads to the cloud. See the [migration patterns and examples overview](#) for a selection of scenarios that use this sample infrastructure as a migration target.

# Best practices to cost and size workloads migrated to Azure

11/9/2020 • 17 minutes to read • [Edit Online](#)

As you plan and design for migration, focusing on costs ensures the long-term success of your Azure migration. During a migration project, it's critical that all teams (such as finance, management, and application development teams) understand associated costs.

- Before migration, it's important to have a baseline for monthly, quarterly, and yearly budget targets in order to estimate the amount you'd spend on your migration and ensure its success.
- After migration, you should optimize costs, continually monitor workloads, and plan for future usage patterns. Migrated resources might start out as one type of workload, but shift to another type over time, based on usage, costs, and shifting business requirements.

This article describes best practices for preparing for and managing cost and size, both before and after migration.

## IMPORTANT

The best practices and opinions described in this article are based on Azure platform and service features available at the time of writing. Features and capabilities change over time. Not all recommendations might be applicable for your deployment, so select what works for you.

## Before migration

Before you move your workloads to the cloud, estimate the monthly cost of running them in Azure. Proactively managing cloud costs helps you adhere to your operating expense budget. If budget is limited, take this into account before migration. Consider converting workloads to Azure serverless technologies, where appropriate, to reduce costs.

The best practices in this section help you:

- Estimate costs.
- Perform right-sizing for virtual machines (VMs) and storage.
- Use Azure Hybrid Benefit.
- Use Azure Reserved Virtual Machine Instances.
- Estimate cloud spending across subscriptions.

## Best practice: Estimate monthly workload costs

To forecast your monthly bill for migrated workloads, there are several tools you can use.

- **Azure pricing calculator:** Select the products you want to estimate, such as VMs and storage. Then, input costs into the calculator to build an estimate.

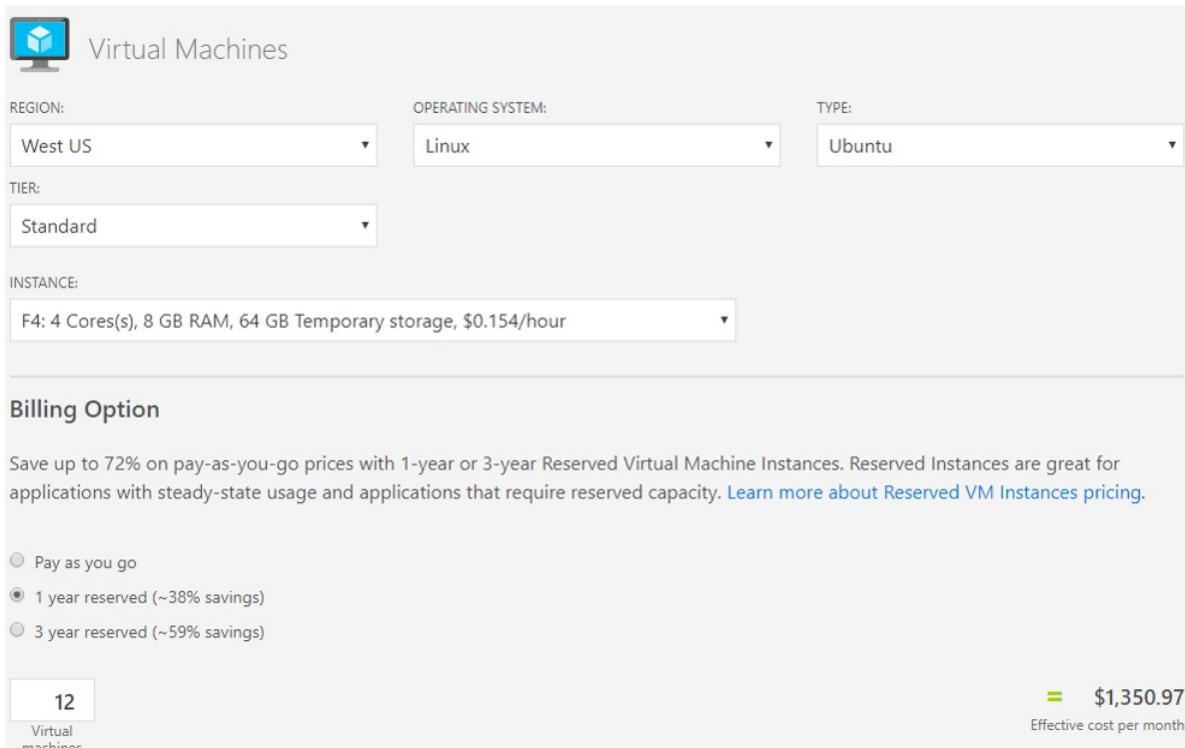


Figure 1: Azure pricing calculator.

- **Azure Migrate:** To estimate costs, you need to review and account for all the resources required to run your workloads in Azure. To acquire this data, you create inventory of your assets, including servers, VMs, databases, and storage. You can use Azure Migrate to collect this information.
  - Azure Migrate discovers and assesses your on-premises environment to provide an inventory.
  - Azure Migrate can map and show you dependencies between VMs, so that you have a complete picture.
  - An Azure Migrate assessment contains estimated cost.
    - **Compute costs:** Using the Azure VM size recommended when you create an assessment, Azure Migrate uses the Azure Billing APIs to calculate estimated monthly VM costs. The estimation considers the operating system, Software Assurance, Azure Reserved Virtual Machine Instances, VM uptime, location, and currency settings. It aggregates the cost across all VMs in the assessment, and calculates a total monthly compute cost.
    - **Storage cost:** Azure Migrate calculates total monthly storage costs by aggregating the storage costs of all VMs in an assessment. You can calculate the monthly storage cost for a specific machine by aggregating the monthly cost of all disks attached to it.

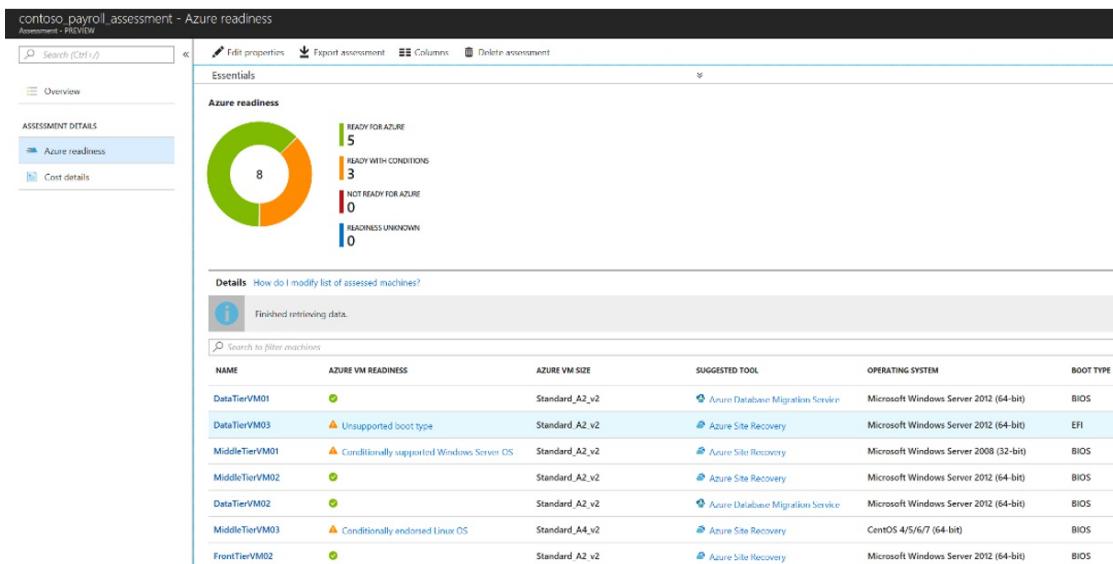


Figure 2: Azure Migrate assessment.

### Learn more:

- Use the [Azure pricing calculator](#).
- Read the [Azure Migrate overview](#).
- Read about [Azure Migrate assessments](#).
- Learn more about [Azure Database Migration Service](#).

## Best practice: Right-size VMs

You can choose various options when you deploy Azure VMs to support workloads. Each VM type has specific features and different combinations of CPU, memory, and disks. VMs are grouped as shown in the following table:

Type	Details	Usage
General-purpose	Balanced CPU-to-memory.	Good for testing and development, small- to medium-sized databases, and low- to medium-volume traffic web servers.
Compute-optimized	High CPU-to-memory.	Good for medium-volume traffic web server, network appliances, batch processes, and application servers.
Memory-optimized	High memory-to-CPU.	Good for relational databases, medium- to large-size cache, and in-memory analytics.
Storage optimized	High disk throughput and I/O.	Good for big data, and SQL and NoSQL databases.
GPU optimized	Specialized VMs. Single or multiple GPUs.	Heavy graphics and video editing.
High performance	Fastest and most powerful CPU. VMs with optional high-throughput network interfaces (RDMA).	Critical high-performance applications.

- It's important to understand the pricing differences between these VMs, and the long-term budget effects.
- Each type has several VM series within it.

- Additionally, when you select a VM within a series, you can only scale the VM up and down within that series. For example, a `DS2_v2` instance can scale up to `DS4_v2`, but it can't be changed to an instance of a different series, such as a `F2s_v2` instance.

#### Learn more:

- Learn more about [VM types and sizing](#), and map sizes to types.
- Plan [sizes for VM instances](#).
- Review a [sample assessment for the fictional Contoso company](#).

## Best practice: Select the right storage

Tuning and maintaining on-premises storage (SAN or NAS), and the networks to support them, can be costly and time-consuming. File (storage) data is commonly migrated to the cloud to help alleviate operational and management headaches. Microsoft provides several options for moving data to Azure, and you need to make decisions about those options. Picking the right storage type for data can save your organization several thousands of dollars every month. Here are a few considerations:

- Data that isn't accessed much and isn't business-critical doesn't need to be placed on the most expensive storage.
- Conversely, important business-critical data should be located on higher tier storage options.
- During migration planning, take an inventory of data and classify it by importance, in order to map it to the most suitable storage. Consider budget and costs, as well as performance. Cost shouldn't necessarily be the main factor. Picking the least expensive option might expose the workload to performance and availability risks.

### Storage data types

Azure provides different types of storage data.

DATA TYPE	DETAILS	USAGE
Blobs	Optimized to store massive amounts of unstructured objects, such as text or binary data.	Access data from everywhere over HTTP/HTTPS.  Use for streaming and random access scenarios. For example, to serve images and documents directly to a browser, stream video and audio, and store backup and disaster recovery data.
Files	Managed file shares accessed over SMB 3.0.	Use when migrating on-premises file shares, and to provide multiple access/connections to file data.
Disks	Based on page blobs.  Disk type: standard (HDD or SSD) or premium (SSD).  Disk management: unmanaged (you manage disk settings and storage) or managed (you select the disk type and Azure manages the disk for you).	Use premium disks for VMs. Use managed disks for simple management and scaling.
Queues	Store and retrieve large numbers of messages accessed via authenticated calls (HTTP or HTTPS).	Connect application components with asynchronous message queueing.

DATA TYPE	DETAILS	USAGE
Tables	Store tables.	This data type is part of Azure Cosmos DB Table API.

## Access tiers

Azure Storage provides different options for accessing block blob data. Selecting the right access tier helps ensure that you store block blob data in the most cost-effective manner.

ACCESS TIER	DETAILS	USAGE
Hot	<p>Higher storage cost than cool. Lower access charges than cool.</p> <p>This is the default tier.</p>	Use for data in active use, that's accessed frequently.
Cool	<p>Lower storage cost than hot. Higher access charges than hot.</p> <p>Store for minimum of 30 days.</p>	Store short-term. Data is available but accessed infrequently.
Archive	<p>Used for individual block blobs.</p> <p>Most cost-effective option for storage. Data access is more expensive than hot and cold.</p>	Use for data that can tolerate several hours of retrieval latency, and will remain in the tier for at least 180 days.

## Storage account types

Azure provides different types of storage accounts and performance tiers.

ACCOUNT TYPE	DETAILS	USAGE
General-purpose v2 standard	<p>Supports blobs (block, page, and append), files, disks, queues, and tables.</p> <p>Supports hot, cool, and archive access tiers. Zone-redundant storage (ZRS) is supported.</p>	Use for most scenarios and most types of data. Standard storage accounts can be HDD- or SSD-based.
General-purpose v2 premium	<p>Supports Blob storage data (page blobs). Supports hot, cool, and archive access tiers. ZRS is supported.</p> <p>Stored on SSD.</p>	Microsoft recommends using for all VMs.
General-purpose v1	Access tiering isn't supported. Doesn't support ZRS.	Use if applications need the Azure classic deployment model.
Blob	<p>Specialized storage account for storing unstructured objects. Provides block blobs and append blobs only (no file, queue, table, or disk storage services).</p> <p>Provides the same durability, availability, scalability and performance as general-purpose v2.</p>	You can't store page blobs in these accounts, and therefore can't store VHD files. You can set an access tier to hot or cool.

## Storage redundancy options

Storage accounts can use different types of redundancy for resilience and high availability.

Type	Details	Usage
Locally redundant storage (LRS)	Protects against a local outage by replicating within a single storage unit to a separate fault domain and update domain. Keeps multiple copies of your data in one datacenter. Provides at least 99.99999999 percent (eleven nines) durability of objects over a particular year.	Consider whether your application stores data that can be easily reconstructed.
Zone-redundant storage (ZRS)	Protects against a datacenter outage by replicating across three storage clusters in a single region. Each storage cluster is physically separated and located in its own Availability Zone. Provides at least 99.9999999999 percent (twelve nines) durability of objects over a particular year, by keeping multiple copies of your data across multiple datacenters or regions.	Consider whether you need consistency, durability, and high availability. Might not protect against a regional disaster, when multiple zones are permanently affected.
Geo-redundant storage (GRS)	Protects against an entire region outage, by replicating data to a secondary region hundreds of miles away from the primary. Provides at least 99.999999999999 percent (sixteen nines) durability of objects over a particular year.	Replica data isn't available unless Microsoft initiates a failover to the secondary region. If failover occurs, read and write access is available.
Read-access geo-redundant storage (RA-GRS)	Similar to GRS. Provides at least 99.999999999999 percent (sixteen nines) durability of objects over a particular year.	Provides 99.99 percent read availability, by allowing read access from the second region used for GRS.

#### Learn more:

- Review [Azure Storage pricing](#).
- Learn about [Azure Import/Export](#).
- Compare [blobs, files, and disk storage data types](#).
- Learn more about [access tiers](#).
- Review [different types of storage accounts](#).
- Learn about [Azure Storage redundancy](#), including LRS, ZRS, GRS, and read-access GRS.
- Learn more about [Azure Files](#).

## Best practice: Take advantage of Azure Hybrid Benefit

A portfolio that integrates on-premises Microsoft software with Azure can provide you with competitive and cost advantages. If you currently have an operating system or other software licensing through Software Assurance, you can take those licenses with you to the cloud, with Azure Hybrid Benefit.

#### Learn more:

- [Take a look at the Azure Hybrid Benefit savings calculator](#).
- Learn more about [Azure Hybrid Benefit for Windows Server](#).
- Review [pricing guidance for SQL Server Azure VMs](#).

## Best practice: Use reserved VM instances

Most cloud platforms use a pay-as-you-go payment model. This model presents disadvantages, because you don't necessarily know how dynamic your workloads will be. When you specify clear intentions for a workload, you contribute to infrastructure planning.

When you use Azure Reserved VM Instances, you prepay for a one-year or three-year term for VM instances.

- Prepayment provides a discount on the resources you use.
- You can significantly reduce VM, Azure SQL Database compute, Azure Cosmos DB, or other resource costs that compare to pay-as-you-go prices.
- Reservations provide a billing discount, and don't affect the runtime state of your resources.
- You can cancel reserved instances.

## Save up to **80%** with RIs and Azure Hybrid Benefit

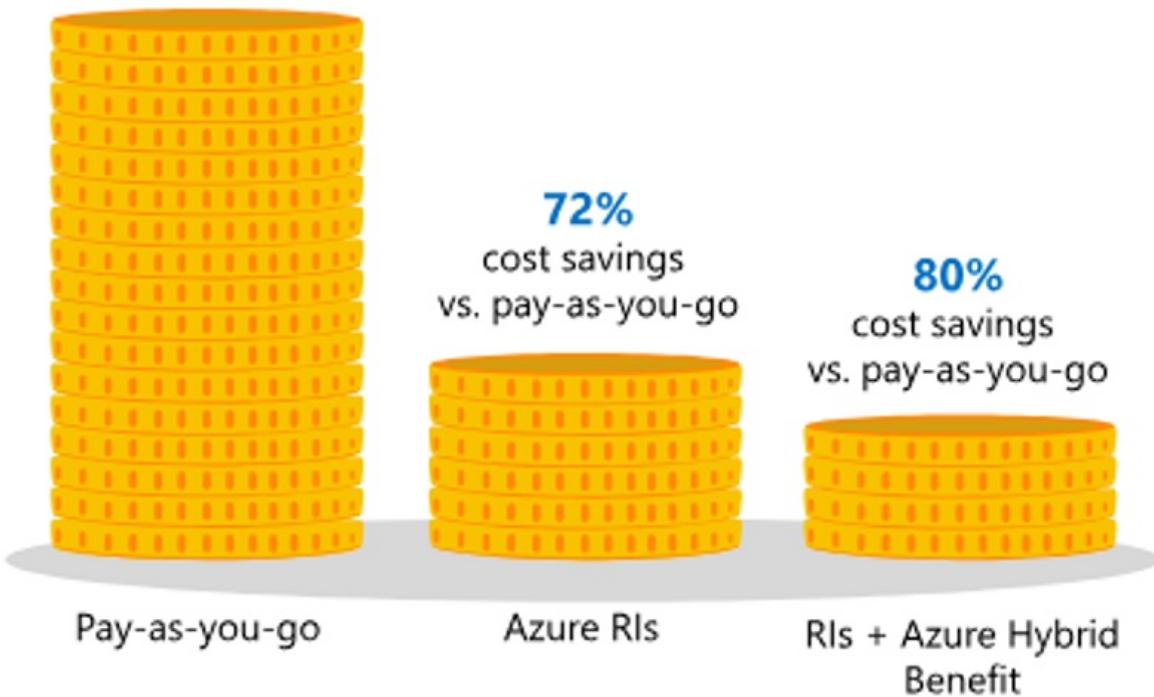


Figure 3: Azure Reserved VM Instances.

### Learn more:

- Learn about [Azure Reservations](#).
- Read the [Azure Reserved VM Instances FAQ](#).
- Review [pricing guidance for SQL Server on Azure VMs](#).

## Best practice: Aggregate cloud spending across subscriptions

Eventually, it's very likely that you'll have more than one Azure subscription. For example, you might need an additional subscription to separate development and production boundaries, or you might have a platform that requires a separate subscription for each client. Having the ability to aggregate data reporting across all the subscriptions into a single platform is a valuable feature.

To do this, you can use Azure Cost Management + Billing APIs. Then, after aggregating data into a single source such as Azure SQL Database, you can use tools like Power BI to surface the aggregated data. You can create aggregated subscription reports, and granular reports. For example, for users who need proactive insights into cost management, you can create specific views of costs, based on department, resource group, or other information. You don't need to provide them with full access to Azure billing data.

#### Learn more:

- Read the [Azure Consumption APIs overview](#).
- Learn how to [connect to Azure Consumption Insights in Power BI Desktop](#).
- Learn how to [manage access to billing information for Azure by using role-based access control \(RBAC\)](#).

## After migration

After a successful migration of your workloads and a few weeks of collecting consumption data, you'll have a clear idea of resources costs. As you analyze data, you can start to generate a budget baseline for Azure resource groups and resources. Then, as you understand where your cloud budget is being spent, you can analyze how to further reduce your costs.

## Best practice: Use Azure Cost Management + Billing

Microsoft provides Azure Cost Management + Billing to help you track spending. This service:

- Helps you to monitor and control Azure spending, and optimize use of resources.
- Reviews your entire subscription and all of its resources, and makes recommendations.
- Provides you with a full API to integrate external tools and financial systems for reporting.
- Tracks resource usage and helps you manage cloud costs with a single, unified view.
- Provides rich operational and financial insights to help you make informed decisions.

With Azure Cost Management + Billing, you can:

- Create a budget for financial accountability.
  - You can account for the services you consume or subscribe to for a specific period (monthly, quarterly, or annually), and a scope (subscriptions or resource groups). For example, you can create an Azure subscription budget for a monthly, quarterly, or annual period.
  - After you create a budget, it's shown in a cost analysis. Viewing your budget against current spending is important when you're analyzing your costs and spending.
  - You can choose to have email notifications sent when your budget thresholds are reached.
  - You can export costs management data to Azure Storage, for analysis.

The screenshot shows the 'Cost Management Demo - Budgets' page. On the left, a sidebar lists various management options like Overview, Access control (IAM), and Cost Management. Under Cost Management, 'Budgets' is selected. The main area displays a table of budgets:

NAME	PERIOD	START D...	END DA...	BUDGET	CURRENT COST	PROGRESS
FY19 Monthly	Monthly	7/1/2018	7/1/2028	\$4,500.00	\$3,508.34	77.96%
FY19 Quarterly	Quarterly	7/1/2018	7/1/2028	\$13,500.00	\$8,461.29	62.68%
FY19	Annually	7/1/2018	7/1/2028	\$54,000.00	\$8,461.29	15.67%

Figure 4: Azure Cost Management + Billing budget.

- Do a cost analysis to explore and analyze your organizational costs, to help you understand how costs are accrued, and identify spending trends.
  - Cost analysis is available to Enterprise Agreement users.
  - You can view cost analysis data for various scopes, including by department, account, subscription, or resource group.
  - You can get a cost analysis that shows total costs for the current month, and accumulated daily costs.

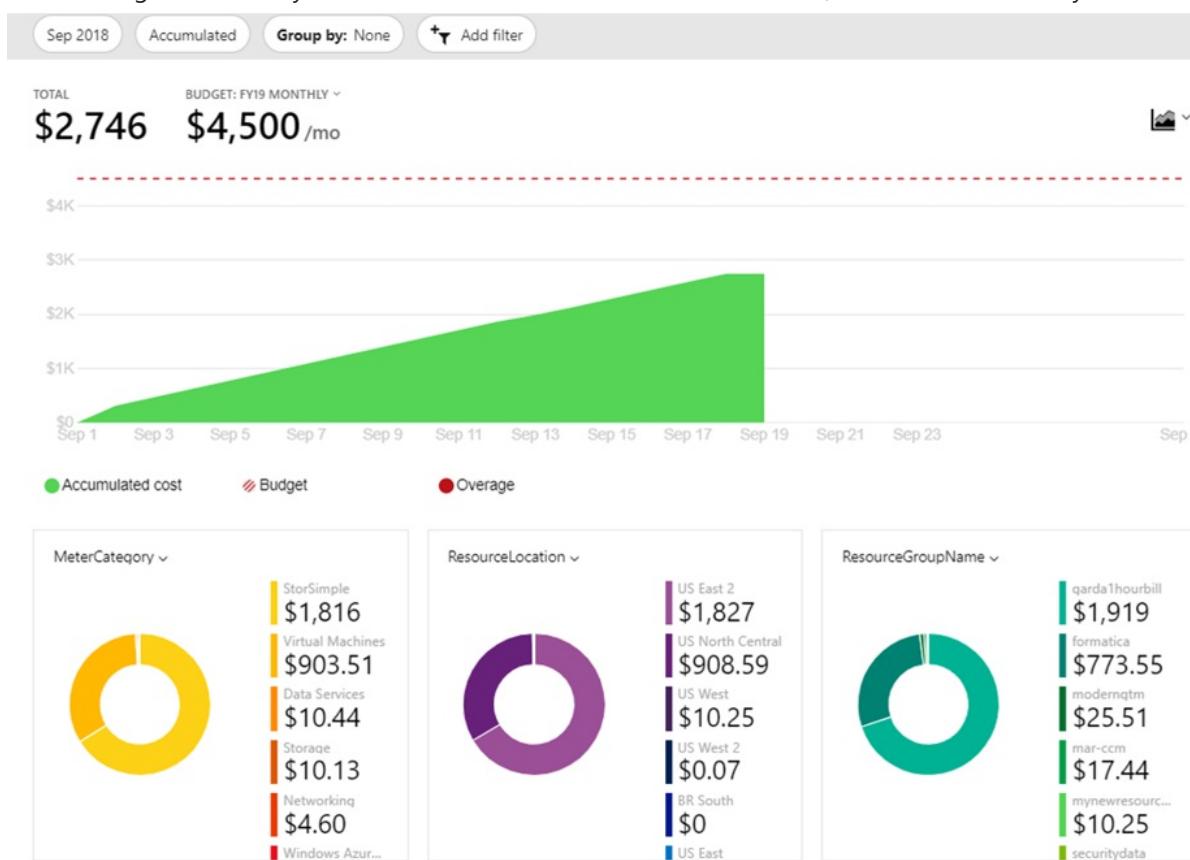


Figure 5: Azure Cost Management + Billing analysis.

- Get Advisor recommendations that show you how you can optimize and improve efficiency.

#### Learn more:

- Read the [Azure Cost Management + Billing overview](#).
- Learn to [optimize your cloud investment with Azure Cost Management + Billing](#).
- Learn about [Azure Cost Management + Billing reports](#).
- Get a [tutorial on optimizing costs from recommendations](#).
- Review the [Azure Consumption APIs](#).

## Best practice: Monitor resource utilization

In Azure you pay for what you use, when resources are consumed, and you don't pay when they aren't. For VMs, billing occurs when a VM is allocated, and you aren't charged after a VM is deallocated. With this in mind, you should monitor VMs in use, and verify VM sizing.

Continually evaluate your VM workloads to determine baselines. For example, if your workload is used heavily Monday through Friday, 8 AM to 6 PM, but hardly used outside those hours, you can downgrade VMs outside peak times. This might mean changing VM sizes, or using virtual machine scale sets to autoscale VMs up or down. Some companies "snooze" VMs via a calendar that specifies when they should be available and when they're not needed.

You can monitor VM usage by using Microsoft tools, such as Azure Cost Management + Billing, Azure Monitor, and Azure Advisor. Third-party tools are also available.

#### NOTE

In addition to VM monitoring, you should monitor other networking resources, such as Azure ExpressRoute and virtual network gateways, for underuse and overuse.

#### Learn more:

- Read overviews of [Azure Monitor](#) and [Azure Advisor](#).
- [Get Azure Advisor cost recommendations](#).
- Learn how to [optimize costs from recommendations](#), and [prevent unexpected charges](#).
- Learn about the [Azure resource optimization \(ARO\) toolkit](#).

## Best practice: Implement resource group budgets

Often, you might find it useful to represent cost boundaries with resource groups. A resource group budget helps you track the costs associated with a resource group. You can trigger alerts and run a wide variety of playbooks when you reach or exceed your budget.

#### Learn more:

- Learn how to [manage costs with Azure budgets](#).
- Review a tutorial on [creating and managing an Azure budget](#).

## Best practice: Optimize Azure Monitor retention

As you move resources into Azure and enable diagnostic logging for them, you generate a lot of log data. Typically, this log data is sent to a storage account that's mapped to a Log Analytics workspace. Here are a few tips for optimizing Azure Monitor retention:

- The longer the log data retention period, the more data you'll have.

- Not all log data is equal, and some resources will generate more log data than others.
- Due to regulations and compliance, it's likely that you'll need to retain log data for some resources longer than for others.
- You should walk a careful line between optimizing your log storage costs, and keeping the log data you need.
- We recommend evaluating and setting up the logging immediately after completing a migration so that you don't spend money on retaining logs of no importance.

**Learn more:**

- Learn about [monitoring usage and estimated costs](#).

## Best practice: Optimize storage

If you followed best practices for selecting storage before migration, you're probably reaping some benefits. But there can be additional storage costs that you can still optimize. Over time, blobs and files become stale. Data might not be used anymore, but regulatory requirements might mean that you need to keep it for a certain period. As such, you might not need to store it on the high-performance storage that you used for the original migration.

Identifying and moving stale data to cheaper storage areas can have a huge impact on your monthly storage budget and cost savings. Azure provides many ways to help you identify and then store this stale data.

- Take advantage of access tiers for general-purpose v2 storage, moving less important data from hot to cool and archived tiers.
- Use StorSimple to help move stale data that's based on customized policies.

**Learn more:**

- Learn more about [access tiers](#).
- Read the [StorSimple overview](#).
- Review [StorSimple pricing](#).

## Best practice: Automate VM optimization

The ultimate goal of running a VM in the cloud is to maximize the CPU, memory, and disk that it uses. If you discover VMs that aren't optimized or have frequent periods when VMs aren't used, it makes sense to either shut them down or downscale them by using virtual machine scale sets.

You can optimize a VM with Azure Automation, virtual machine scale sets, auto-shutdown, and scripted or third-party solutions.

**Learn more:**

- Learn about [vertical autoscaling](#).
- [Schedule a VM autostart](#).
- Learn how to [start or stop VMs off hours in Azure Automation](#).
- Get more information about [Azure Advisor](#), and the [Azure resource optimization \(ARO\) toolkit](#).

## Best practices: Use Azure Logic Apps and runbooks with Budgets API

Azure provides a REST API that has access to your tenant billing information. You can use the Budgets API to integrate external systems and workflows that are triggered by metrics that you build from the API data. You can pull usage and resource data into your preferred data analysis tools. You can integrate the Budgets API with Azure Logic Apps and runbooks.

The Azure Resource Usage and RateCard APIs can help you accurately predict and manage your costs. The APIs

are implemented as a resource provider and are included in the APIs exposed by the Azure Resource Manager.

**Learn more:**

- Review the [Azure Budgets API](#).
- Get insights into usage with the [Azure Billing APIs](#).

## Best practice: Implement serverless technologies

VM workloads are often migrated "as-is" to avoid downtime. Often, VMs can host tasks that are intermittent, run over a short period, or alternately, take up many hours. Examples include VMs that run scheduled tasks, such as Windows task scheduler or PowerShell scripts. When these tasks aren't running, you're nevertheless absorbing VM and disk storage costs.

After migrating and thoroughly reviewing these types of tasks, you might consider migrating them to serverless technologies like Azure Functions or Azure Batch jobs. These solutions can cut costs, and you'd no longer need to manage and maintain the VMs.

**Learn more:**

- Learn about [Azure Functions](#).
- Learn about [Azure Batch](#).

## Next steps

Review other best practices:

- [Best practices for security and management](#) after migration.
- [Best practices for networking](#) after migration.

# Scale a migration to Azure

11/9/2020 • 20 minutes to read • [Edit Online](#)

This article demonstrates how the fictional company Contoso performs a migration at scale to Azure. The company considers how to plan and perform a migration of more than 3,000 workloads, 8,000 databases, and 10,000 virtual machines (VMs).

## Business drivers

The IT leadership team has worked closely with business partners to understand what they want to achieve with this migration:

- **Address business growth.** Contoso is growing, causing pressure on on-premises systems and infrastructure.
- **Increase efficiency.** Contoso needs to remove unnecessary procedures, and streamline processes for developers and users. The business needs IT to be fast and not waste time or money, thus delivering faster on customer requirements.
- **Increase agility.** Contoso IT needs to be more responsive to the needs of the business. It must be able to react faster than the changes in the marketplace, to enable success in a global economy. It mustn't get in the way or become a business blocker.
- **Scale.** As the business grows successfully, the Contoso IT team must provide systems that are able to grow at the same pace.
- **Improve cost models.** Contoso wants to lessen capital requirements in the IT budget. Contoso wants to use cloud abilities to scale and reduce the need for expensive hardware.
- **Lower licensing costs.** Contoso wants to minimize cloud costs.

## Migration goals

The Contoso cloud team has pinned down goals for this migration. It used these goals to determine the best migration method.

REQUIREMENTS	DETAILS
Move to Azure quickly	Contoso wants to start moving applications and VMs to Azure as quickly as possible.
Compile a full inventory	Contoso wants a complete inventory of all applications, databases, and VMs in the organization.
Assess and classify applications	Contoso wants to take full advantage of the cloud. As a default, Contoso assumes that all services will run as platform as a service (PaaS). Infrastructure as a service (IaaS) will be used where PaaS isn't appropriate.
Train and move to DevOps	Contoso wants to move to a DevOps model. Contoso will provide Azure and DevOps training and will reorganize teams as necessary.

After establishing goals and requirements, Contoso reviews the IT footprint and identifies the migration process.

## Current deployment

Contoso has planned and set up an [Azure infrastructure](#) and tried out different proof-of-concept (POC) migration combinations as detailed in the preceding table. It's now ready to embark on a full migration to Azure at scale. Here's what Contoso wants to migrate.

ITEM	VOLUME	DETAILS
Workloads	> 3,000 Applications	<ul style="list-style-type: none"><li>Applications run on VMs.</li><li>Application platforms include Windows, SQL Server, and <a href="#">LAMP</a>.</li></ul>
Databases	Approximately 8,500 databases	Databases include SQL Server, MySQL, and PostgreSQL.
VMs	> 35,000 VMs	VMs run on VMware hosts and are managed by vCenter servers.

## Migration process

Now that Contoso has established business drivers and migration goals, it can align to the [Migrate methodology](#). It can build on the application of migration waves and migration sprints to iteratively plan and execute migration efforts.

## Plan

Contoso kicks off the planning process by discovering and assessing on-premises applications, data, and infrastructure. Here's what Contoso will do:

- Contoso needs to discover applications, map dependencies across applications, and decide on migration order and priority.
- As Contoso assesses, it will build out a comprehensive inventory of applications and resources. Along with the new inventory, Contoso will use and update these existing items:
  - The configuration management database (CMDB). It holds technical configurations for Contoso applications.
  - The service catalog. It documents the operational details of applications, including associated business partners and service-level agreements.

### Discover applications

Contoso runs thousands of applications across a range of servers. In addition to the CMDB and service catalog, Contoso needs discovery and assessment tools.

The tools must provide a mechanism that can feed assessment data into the migration process. Assessment tools must provide data that helps build up an intelligent inventory of Contoso's physical and virtual resources. Data should include profile information and performance metrics.

When discovery is complete, Contoso should have a full inventory of assets and the metadata associated with them. The company will use this inventory to define the migration plan.

### Identify classifications

Contoso identifies some common categories to classify assets in the inventory. These classifications are critical to Contoso's decision making for migration. The classification list helps to establish migration priorities and identify complex issues.

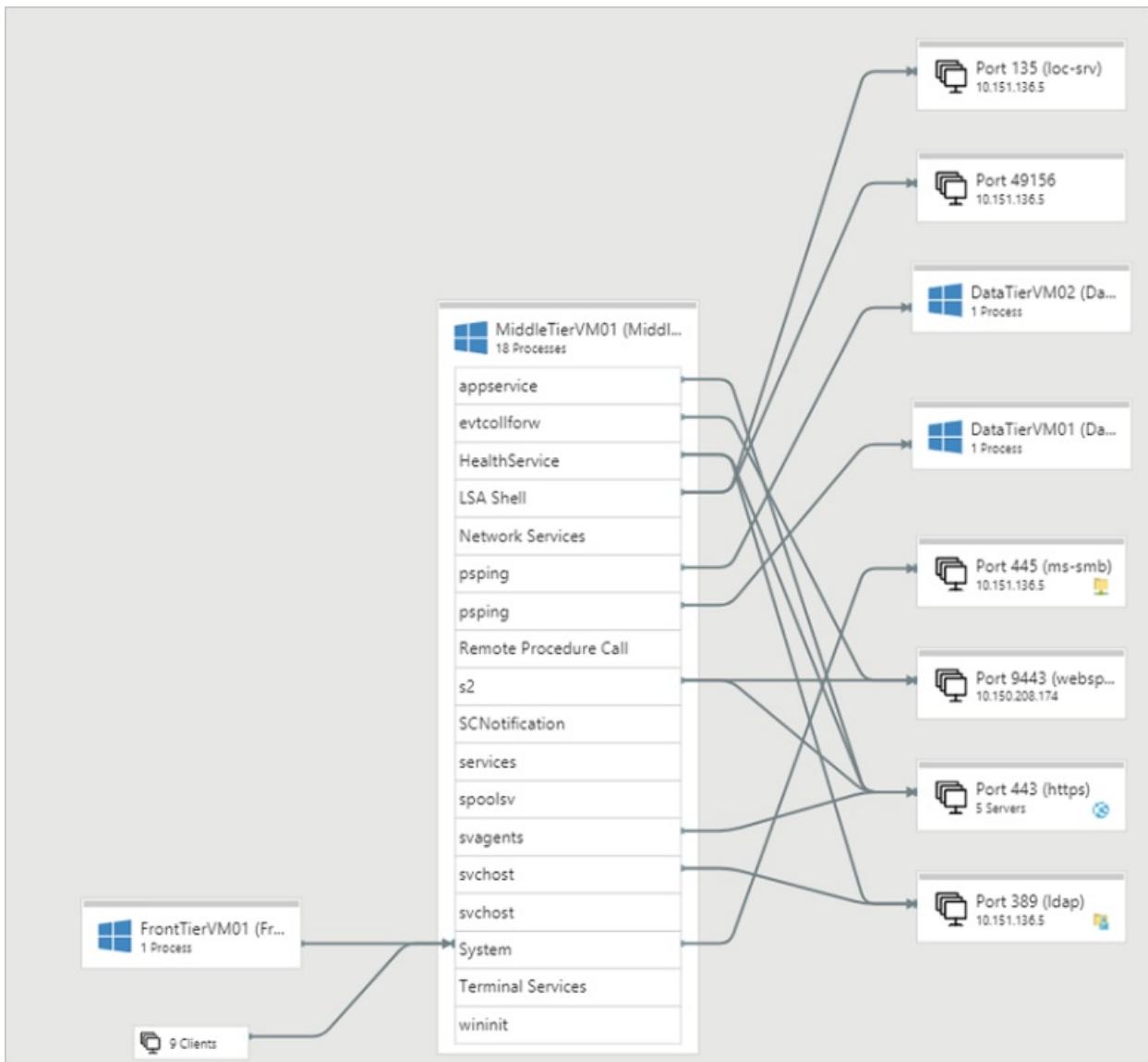
CATEGORY	ASSIGNED VALUE	DETAILS
Business group	List of business group names	Which group is responsible for the inventory item?
POC candidate	Y/N	Can the application be used as a POC or early adopter for cloud migration?
Technical debt	None/Some/Severe	Is the inventory item running or using an out-of-support product, platform, or operating system?
Firewall implications	Y/N	Does the application communicate with the internet or outside traffic? Does it integrate with a firewall?
Security issues	Y/N	Are there known security issues with the application? Does the application use unencrypted data or out-of-date platforms?

### Discover application dependencies

As part of the assessment process, Contoso needs to identify where applications are running. It also needs to figure out the dependencies and connections between application servers. Contoso maps the environment in steps:

1. Contoso discovers how servers and machines map to individual applications, network locations, and groups.
2. Contoso clearly identifies applications that have few dependencies and are suitable for a quick migration.
3. Contoso can use mapping to help identify more complex dependencies and communications between application servers. Contoso can then group these servers logically to represent applications and plan a migration strategy based on these groups.

With mapping completed, Contoso can ensure that all application components are identified and accounted for when building the migration plan.



## Evaluate applications

As the last step in the discovery and assessment process, Contoso can evaluate assessment and mapping results to figure out how to migrate each application in the service catalog.

To capture this evaluation process, Contoso adds a couple of classifications to the inventory.

CATEGORY	ASSIGNED VALUE	DETAILS
Business group	List of business group names	Which group is responsible for the inventory item?
POC candidate	Y/N	Can the application be used as a POC or early adopter for cloud migration?
Technical debt	None/Some/Severe	Is the inventory item running or using an out-of-support product, platform, or operating system?
Firewall implications	Y/N	Does the application communicate with the internet or outside traffic? Does it integrate with a firewall?

CATEGORY	ASSIGNED VALUE	DETAILS
Security issues	Y/N	Are there known security issues with the application? Does the application use unencrypted data or out-of-date platforms?
Migration strategy	Rehost/Refactor/Rearchitect/Rebuild	What kind of migration is needed for the application? How will the application be deployed in Azure? <a href="#">Learn more</a> .
Technical complexity	1-5	How complex is the migration? This value should be defined by Contoso DevOps and relevant partners.
Business criticality	1-5	How important is the application for the business? For example, a small workgroup application might be assigned a score of one, while a critical application used across the organization might be assigned a score of five. This score will affect the migration priority level.
Migration priority	1/2/3	What's the migration priority for the application?
Migration risk	1-5	What's the risk level for migrating the application? Contoso DevOps and relevant partners should agree on this value.

## Determine costs

To determine costs and the potential savings of Azure migration, Contoso can use the [total cost of ownership \(TCO\) calculator](#) to calculate and compare the TCO for Azure to a comparable on-premises deployment.

## Identify assessment tools

Contoso decides which tool to use for discovery, assessment, and building the inventory. Contoso identifies a mix of Azure tools and services, native application tools and scripts, and partner tools. In particular, Contoso is interested in how Azure Migrate can be used to assess at scale.

### Azure Migrate

The Azure Migrate service helps you to discover and assess on-premises VMware VMs, in preparation for migration to Azure. Here's what Azure Migrate does:

#### 1. Discover: Discover on-premises VMware VMs.

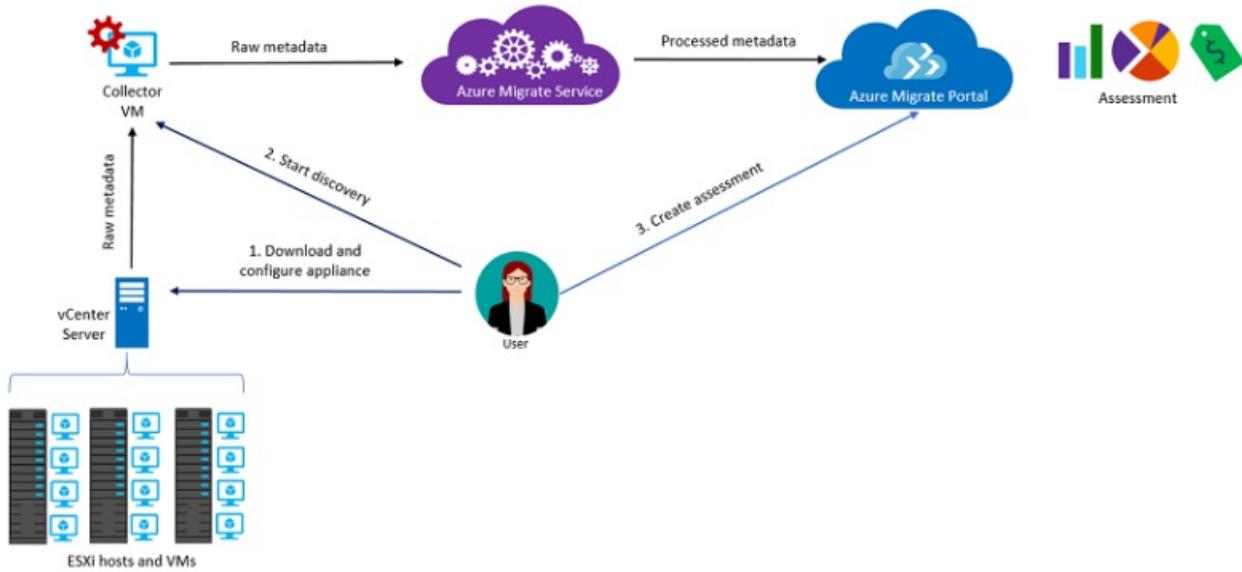
Azure Migrate supports discovery from multiple vCenter servers (serially) and can run discoveries in separate Azure Migrate projects.

Azure Migrate performs discovery via a VMware VM running the Azure Migrate Collector. The same collector can discover VMs on different vCenter servers and send data to different projects.

#### 2. Assess readiness: Assess whether on-premises machines are suitable for running in Azure. An assessment includes:

- **Size recommendations:** Get size recommendations for Azure VMs, based on the performance history of on-premises VMs.

- **Estimated monthly costs:** Get estimated costs for running on-premises machines in Azure.
3. **Identify dependencies:** Visualize dependencies of on-premises machines to create optimal machine groups for assessment and migration.



Contoso needs to use Azure Migrate correctly, given the scale of this migration:

- Contoso does an app-by-app assessment with Azure Migrate. This assessment ensures that Azure Migrate returns timely data to the Azure portal.
- Contoso admins learn how to [deploy Azure Migrate at scale](#).
- Contoso notes the Azure Migrate limits summarized in the following table.

ACTION	LIMIT
Create Azure Migrate project	10,000 VMs
Discovery	10,000 VMs
Assessment	10,000 VMs

Contoso will use Azure Migrate as follows:

- In vCenter, organize VMs into folders. This will make it easy for the admins to focus as they run an assessment against VMs in a specific folder.
- Assess dependencies between machines. This requires agents to be installed on VMs to be assessed.

Contoso will use automated scripts to install the required Windows or Linux agents. By scripting, Contoso can push the installation to VMs within a vCenter folder.

#### Database tools

In addition to Azure Migrate, Contoso will focus on using tools specifically for database assessment. Tools such as [Data Migration Assistant](#) will help assess SQL Server databases for migration.

Data Migration Assistant can help Contoso to figure out whether on-premises databases are compatible with a range of Azure database solutions. These solutions include Azure SQL Database, SQL Server running on an Azure IaaS VM, and Azure SQL Managed Instance.

In addition to Database Migration Service, Contoso has some scripts that it uses to discover and document the SQL Server databases. These scripts are located in the GitHub repo.

## Partner assessment tools

There are several other partner tools that can help Contoso in assessing the on-premises environment for migration to Azure. Learn more about [Azure migration partners](#).

# Phase 2: Migrate

With the assessment complete, Contoso needs to identify tools to move its applications, data, and infrastructure to Azure.

## Migration strategies

Contoso can consider four broad migration strategies.

STRATEGY	DETAILS	USAGE
Rehost	<ul style="list-style-type: none"><li>Often called a <i>lift-and-shift</i> migration, this is a no-code option for migrating existing applications to Azure quickly.</li><li>An application is migrated as is with the benefits of the cloud and without the risks or costs associated with code changes.</li></ul>	<ul style="list-style-type: none"><li>Contoso can rehost less-strategic applications that require no code changes.</li></ul>
Refactor	<ul style="list-style-type: none"><li>Also called <i>repackaging</i>, this strategy requires minimal application code or configuration changes to connect the application to Azure PaaS, and take better advantage of cloud capabilities.</li></ul>	<ul style="list-style-type: none"><li>Contoso can refactor strategic applications to retain the same basic functionality, but move them to run on an Azure platform such as Azure App Service.</li><li>This requires minimum code changes.</li><li>On the other hand, Contoso will have to maintain a VM platform because Microsoft won't manage this.</li></ul>
Rearchitect	<ul style="list-style-type: none"><li>This strategy modifies or extends an application code base to optimize the application architecture for cloud capabilities and scale.</li><li>It modernizes an application into a resilient, highly scalable, independently deployable architecture.</li><li>Azure services can accelerate the process, scale applications with confidence, and manage applications with ease.</li></ul>	
Rebuild	<ul style="list-style-type: none"><li>This approach rebuilds an application from scratch by using cloud-native technologies.</li><li>Azure PaaS provides a complete development and deployment environment in the cloud. It eliminates some expense and complexity of software licenses. It also removes the need for an underlying application infrastructure, middleware, and other resources.</li></ul>	<ul style="list-style-type: none"><li>Contoso can rewrite critical applications to take advantage of cloud technologies such as serverless compute or microservices.</li><li>Contoso will manage the application and services that it develops, and Azure will manage everything else.</li></ul>

Data must also be considered, especially with the volume of databases that Contoso has. Contoso's default approach is to use PaaS services such as Azure SQL Database to take full advantage of cloud features. By moving to a PaaS service for databases, Contoso will only have to maintain data. It will leave the underlying platform to Microsoft.

## Evaluate migration tools

Contoso is primarily using these Azure services and tools for the migration:

- [Azure Migrate](#): Service for migrating on-premises virtual machines and other resources to Azure.
- [Azure Database Migration Service](#): Migrates on-premises databases such as SQL Server, MySQL, and Oracle to Azure.

### Azure Migrate

Azure Migrate is the primary Azure service for orchestrating migration from within Azure and from on-premises sites to Azure.

Azure Migrate orchestrates replication from on-premises locations to Azure. When replication is set up and running, on-premises machines can be failed over to Azure, completing the migration.

Contoso already [completed a POC](#) to see how Azure Migrate can help it to migrate to the cloud.

#### Use Azure Migrate at scale

Contoso plans to perform multiple lift-and-shift migrations. To ensure that this works, Azure Migrate will replicate batches of around 100 VMs at a time. To determine how this will work, Contoso must perform capacity planning for the proposed migration.

Contoso needs to gather information about their traffic volumes. In particular:

- It needs to determine the rate of change for VMs that it wants to replicate.
- It needs to take network connectivity from the on-premises site to Azure into account.

In response to capacity and volume requirements, Contoso will need to allocate sufficient bandwidth based on the daily data change rate for the required VMs, to meet its recovery point objective (RPO). Last, it must determine how many servers are needed to run the Azure Migrate components for the deployment.

#### Gather on-premises information

Contoso can use Azure Migrate:

- To remotely profile VMs without an impact on the production environment. This helps pinpoint bandwidth and storage requirements for replication and failover.
- Without installing any Site Recovery components on-premises.

The tool gathers information about compatible and incompatible VMs, disks per VM, and data churn per disk. It also identifies network bandwidth requirements and the Azure infrastructure needed for successful replication and failover.

Contoso needs to ensure that it runs the planner tool on a Windows Server machine that matches the minimum requirements for the Site Recovery configuration server. The configuration server is a Site Recovery machine that's needed to replicate on-premises VMware VMs.

#### Identify Site Recovery requirements

In addition to the VMs being replicated, Site Recovery requires several components for VMware migration.

COMPONENT	DETAILS
Configuration server	<ul style="list-style-type: none"><li>● Usually a VMware VM configured through an OVF template.</li><li>● The configuration server component coordinates communications between on-premises and Azure, and it manages data replication.</li></ul>

COMPONENT	DETAILS
Process server	<ul style="list-style-type: none"> <li>Installed by default on the configuration server.</li> <li>The process server component receives replication data; optimizes it with caching, compression, and encryption; and sends it to Azure Storage.</li> <li>The process server also installs the Azure Site Recovery Mobility service on VMs that you want to replicate, and performs automatic discovery of on-premises machines.</li> <li>Scaled deployments need additional, standalone process servers to handle large volumes of replication traffic.</li> </ul>
Mobility service	<ul style="list-style-type: none"> <li>The Mobility service agent is installed on each VMware VM that will be migrated with Azure Site Recovery.</li> </ul>

Contoso needs to figure out how to deploy these components, based on capacity considerations.

COMPONENT	CAPACITY REQUIREMENTS
Maximum daily change rate	<ul style="list-style-type: none"> <li>A single process server can handle a daily change rate up to 2 terabytes (TB). Because a VM can only use one process server, the maximum daily data change rate that's supported for a replicated VM is 2 TB.</li> </ul>
Maximum throughput	<ul style="list-style-type: none"> <li>A standard Azure Storage account can handle a maximum of 20,000 requests per second. I/O operations per second (IOPS) across a replicating VM should be within this limit. For example, if a VM has 5 disks, and each disk generates 120 IOPS (8K size) on the VM, then it will be within the Azure per-disk IOPS limit of 500.</li> <li>The number of storage accounts needed equals the total source machine IOPS divided by 20,000. A replicated machine can belong to only a single storage account in Azure.</li> </ul>
Configuration server	<p>Based on Contoso's estimate of replicating 100 to 200 VMs together and the <a href="#">configuration server sizing requirements</a>, Contoso estimates that it needs the following type of server machine configuration:</p> <ul style="list-style-type: none"> <li>CPU: 16 vCPUs (2 sockets × 8 cores @ 2.5 GHz)</li> <li>Memory: 32 GB</li> <li>Cache disk: 1 TB</li> <li>Data change rate: 1 to 2 TB</li> </ul> <p>In addition to sizing requirements, Contoso must ensure that the configuration server is optimally located on the same network and LAN segment as the VMs to be migrated.</p>
Process server	<p>Contoso will deploy a standalone dedicated process server with the ability to replicate 100 to 200 VMs:</p> <ul style="list-style-type: none"> <li>CPU: 16 vCPUs (2 sockets × 8 cores @ 2.5 GHz)</li> <li>Memory: 32 GB</li> <li>Cache disk: 1 TB</li> <li>Data change rate: 1 to 2 TB</li> </ul> <p>The process server will be working hard, so it's located on an ESXi host that can handle the disk I/O, network traffic, and CPU required for the replication. Contoso will consider a dedicated host for this purpose.</p>

COMPONENT	CAPACITY REQUIREMENTS
Networking	<ul style="list-style-type: none"> <li>Contoso has reviewed the current site-to-site VPN infrastructure and decided to implement Azure ExpressRoute. The implementation is critical because it will lower latency and improve bandwidth to Contoso's primary Azure region (<a href="#">East US 2</a>).</li> <li>Contoso will need to carefully monitor data flowing from the process server. If the data overloads the network bandwidth, Contoso will consider <a href="#">throttling the process server bandwidth</a>.</li> </ul>
Azure Storage	<ul style="list-style-type: none"> <li>For migration, Contoso must identify the right type and number of target Azure Storage accounts. Site Recovery replicates VM data to Azure Storage.</li> <li>Site Recovery can replicate to standard or premium SSD storage accounts.</li> <li>To decide about storage, Contoso must review <a href="#">storage limits</a> and consider expected growth and future increased usage. Given the speed and priority of migrations, Contoso has decided to use premium SSDs.</li> <li>Contoso has decided to use managed disks for all VMs deployed to Azure. The IOPS required will help determine if the disks will be standard HDD, standard SSD, or premium SSD.</li> </ul>

#### Azure Database Migration Service

Azure Database Migration Service is a fully managed service that enables seamless migrations from multiple database sources to Azure data platforms with minimal downtime. Here are some details about the service:

- It integrates functionality of existing tools and services. It uses Data Migration Assistant to generate assessment reports that pinpoint recommendations about database compatibility and any required modifications.
- It uses a simple, self-guided migration process with intelligent assessment that helps address potential issues before the migration.
- It can migrate at scale from multiple sources to the target Azure database.
- It provides support from SQL Server 2005 to SQL Server 2017.

Database Migration Service isn't the only Microsoft database migration tool. Get a [comparison of tools and services](#).

#### Use Database Migration Service at scale

Contoso will use Database Migration Service when migrating from SQL Server.

When provisioning Database Migration Service, Contoso needs to size it correctly and set it to optimize performance for data migrations. Contoso will select the Business Critical tier with four vCores. This option allows the service to take advantage of multiple vCPUs for parallelization and faster data transfer.

<b>General Purpose</b> For offline migrations with downtime 1 vCores, 2 vCores, 4 vCores	<b>Business Critical [Preview]</b> For offline and online migrations with minimal downtime 4 vCores
--	---

**vCores** [How to choose the right vCores?](#)

4 vCores

Another scaling tactic that Contoso can use is to temporarily scale up the Azure SQL Database or Azure Database for MySQL target instance to the Premium pricing tier during data migration. This minimizes database throttling that might affect data transfer activities when an organization is using lower tiers.

#### Use other tools

In addition to Database Migration Service, Contoso can use other tools and services to identify VM information:

- Scripts to help with manual migrations. These are available in the GitHub repo.
- Various [partner tools](#) for migration.

## Ready for production

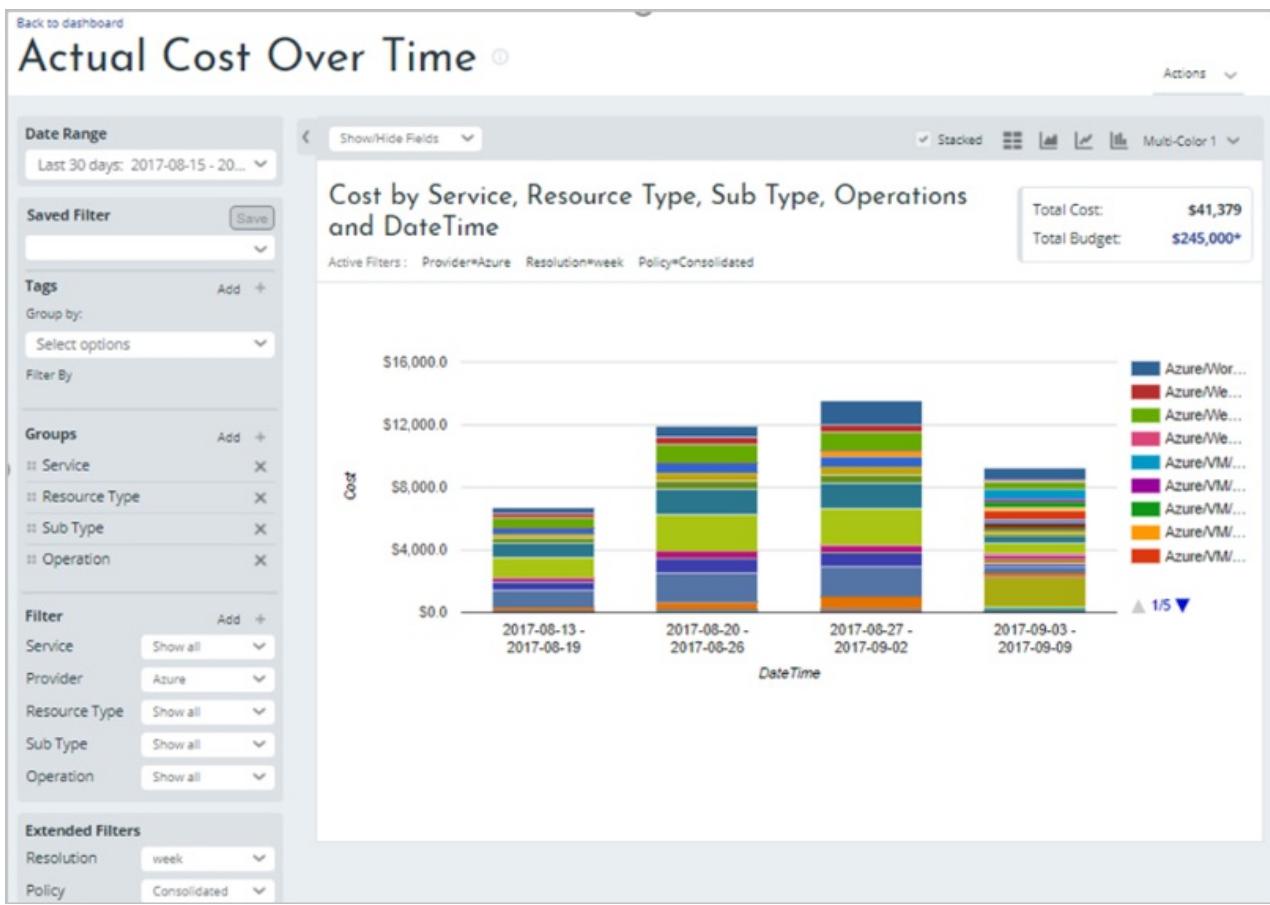
After Contoso moves resources to Azure, it needs to streamline them to improve performance, and maximize ROI with cost management tools. Because Azure is a pay-for-use service, it's critical for Contoso to understand how systems are performing and to ensure they're sized properly.

### Azure Cost Management and Billing

To make the most of their cloud investment, Contoso will take advantage of the free Azure Cost Management and Billing tool. This solution allows Contoso to manage cloud spending with transparency and accuracy. It provides tools to monitor, allocate, and trim cloud costs.

Azure Cost Management and Billing provides simple dashboard reports to help with cost allocation, showbacks, and chargebacks. The tool can help optimize cloud spending by identifying underutilized resources that Contoso can then manage and adjust.

You can learn more in an [overview of Azure Cost Management and Billing](#).



## Native tools

Contoso will also use scripts to locate unused resources.

During large migrations, there are often leftover pieces of data such as virtual hard drives, which incur a charge but provide no value to the company. Scripts are available in [the GitHub repo](#).

Contoso will take advantage of work done by Microsoft's IT department and consider implementing the Azure Resource Optimization (ARO) toolkit. The toolkit is also in the GitHub repo.

Contoso can deploy an Azure Automation account with preconfigured runbooks and schedules to its subscription, and start saving money. Resource optimization happens automatically on a subscription after a schedule is enabled or created, including optimization on new resources. This provides decentralized automation capabilities to reduce costs. Features include:

- Autosnooze Azure VMs based on low CPU utilization.
- Schedule Azure VMs to snooze and unsnooze.
- Schedule Azure VMs to snooze or unsnooze in ascending and descending order by using Azure tags.
- Bulk-delete resource groups on demand.

## Partner optimization tools

Contoso can use partner tools such as [Hanu](#) and [Scalr](#).

## Phase 4: Secure and manage

In this phase, Contoso uses Azure security and management resources to govern, secure, and monitor cloud applications in Azure. These resources help an organization run a secure and well-managed environment while using products available in the Azure portal.

Contoso begins using these services during migration. With Azure hybrid support, Contoso continues using many of them for a consistent experience across the hybrid cloud.

## Security

Contoso will rely on Azure Security Center for unified security management and Azure Advanced Threat Protection across hybrid cloud workloads.

Security Center provides full visibility into and control over the security of cloud applications in Azure. Contoso can quickly detect and take action in response to threats, and reduce security exposure by enabling adaptive threat protection.

[Learn more](#) about Security Center.

## Monitoring

Contoso needs visibility into the health and performance of the newly migrated applications, infrastructure, and data now running in Azure. Contoso will use built-in Azure cloud monitoring tools such as Azure Monitor, a Log Analytics workspace, and Application Insights.

By using these tools, Contoso can easily collect data from sources and gain insights. For example, Contoso can gauge CPU disk and memory utilization for VMs, view applications and network dependencies across multiple VMs, and track application performance. Contoso will use these cloud monitoring tools to take action and integrate with service solutions.

Learn more about [Azure monitoring](#).

## Business continuity and disaster recovery

Contoso will need a business continuity and disaster recovery (BCDR) strategy for its Azure resources.

Azure provides [built-in BCDR features](#) to help protect data and keep applications and services running.

In addition to built-in features, Contoso wants to ensure that it can recover from failures, avoid costly business disruptions, meet compliance goals, and protect data against ransomware and human errors. To do this:

- Contoso will deploy Azure Backup as a cost-efficient solution for backup of Azure resources. Because it's built in, Contoso can set up cloud backups in a few simple steps.
- Contoso will set up disaster recovery for Azure VMs by using Azure Site Recovery for replication, failover, and fallback between Azure regions that it specifies. This ensures that applications running on Azure VMs remain available in a secondary region of Contoso's choosing if an outage occurs in the primary region. [Learn more](#).

## Conclusion

In this article, Contoso planned for an Azure migration at scale. It divided the migration process into four stages. The stages ran from assessment and migration, through to optimization, security, and management after migration was complete.

It's important for an organization to plan a migration project as a whole process and to migrate its systems by breaking down sets into classifications and numbers that make sense for the business. By assessing data and applying classifications, projects can be broken down into a series of smaller migrations, which can run safely and rapidly. The sum of these smaller migrations quickly turns into a large successful migration to Azure.

# Data definition languages for schema migration

11/9/2020 • 23 minutes to read • [Edit Online](#)

This article describes design considerations and performance options for data definition languages (DDLs) when you're migrating schemas to Azure Synapse Analytics.

## Design considerations

### Preparation for migration

When you're preparing to migrate existing data to Azure Synapse Analytics, it's important to clearly define the scope of the exercise (especially for an initial migration project). The time spent up front to understand how database objects and related processes will migrate can reduce both effort and risk later in the project.

Create an inventory of database objects to be migrated. Depending on the source platform, this inventory will include some or all of the following objects:

- Tables
- Views
- Indexes
- Functions
- Stored procedures
- Data distribution and partitioning

The basic information for these objects should include metrics such as row counts, physical size, data compression ratios, and object dependencies. This information should be available via queries against system catalog tables in the source system. The system metadata is the best source for this information. External documentation might be stale and not in sync with changes that have been applied to the data structure since the initial implementation.

You might also be able to analyze actual object usage from query logs or use tooling from Microsoft partners, such as Attunity Visibility, to help. It's possible that some tables don't need to be migrated because they're no longer used in production queries.

Data size and workload information is important for Azure Synapse Analytics because it helps to define appropriate configurations. One example is the required levels of concurrency. Understanding the expected growth of data and workloads might affect a recommended target configuration, and it's a good practice to also harness this information.

When you're using data volumes to estimate the storage required for the new target platform, it's important to understand the data compression ratio, if any, on the source database. Simply taking the amount of storage used on the source system is likely to be a false basis for sizing. Monitoring and metadata information can help you determine uncompressed raw data size and overheads for indexing, data replication, logging, or other processes in the current system.

The uncompressed raw data size of the tables to be migrated is a good starting point for estimating the storage required in the new target Azure Synapse Analytics environment.

The new target platform will also include a compression factor and indexing overhead, but these will probably be different from the source system. Azure Synapse Analytics storage pricing also includes seven days of snapshot backups. When compared to the existing environment, this can have an impact on the overall cost of storage required.

You can delay performance tuning for the data model until late in the migration process and time this with when

real data volumes are in the data warehouse. However, we recommend that you implement some performance tuning options earlier on.

For example, in Azure Synapse Analytics, it makes sense to define small dimension tables as replicated tables and to define large fact tables as clustered columnstore indexes. Similarly, indexes defined in the source environment provide a good indication of which columns might benefit from indexing in the new environment. Using this information when you're initially defining the tables before loading will save time later in the process.

It's good practice to measure the compression ratio and index overhead for your own data in Azure Synapse Analytics as the migration project progresses. This measure enables future capacity planning.

It might be possible to simplify your existing data warehouse before migration by reducing complexity to ease migration. This effort might include:

- Removing or archiving unused tables before migrating to avoid migrating data that's not used. Archiving to Azure Blob storage and defining the data as an external table might keep the data available for a lower cost.
- Converting physical data marts to virtual data marts by using data virtualization software to reduce what you have to migrate. This conversion also improves agility and reduces total cost of ownership. You might consider it as modernization during migration.

One objective of the migration exercise might also be to modernize the warehouse by changing the underlying data model. One example is moving from an Inmon-style data model to a data vault approach. You should decide this as part of the preparation phase and incorporate a strategy for the transition into the migration plan.

The recommended approach in this scenario is to first migrate the data model as is to the new platform and then transition to the new model in Azure Synapse Analytics. Use the platform's scalability and performance characteristics to execute the transformation without affecting the source system.

### **Data model migration**

Depending on the platform and the origins of the source system, the data model of some or all parts may already be in a star or snowflake schema form. If so, you can directly migrate it to Azure Synapse Analytics as is. This scenario is the easiest and lowest-risk migration to achieve. An as-is migration can also be the first stage of a more complex migration that includes a transition to a new underlying data model such as a data vault, as described earlier.

Any set of relational tables and views can be migrated to Azure Synapse Analytics. For analytical query workloads against a large data set, a star or snowflake data model generally gives the best overall performance. If the source data model is not already in this form, it might be worth using the migration process to reengineer the model.

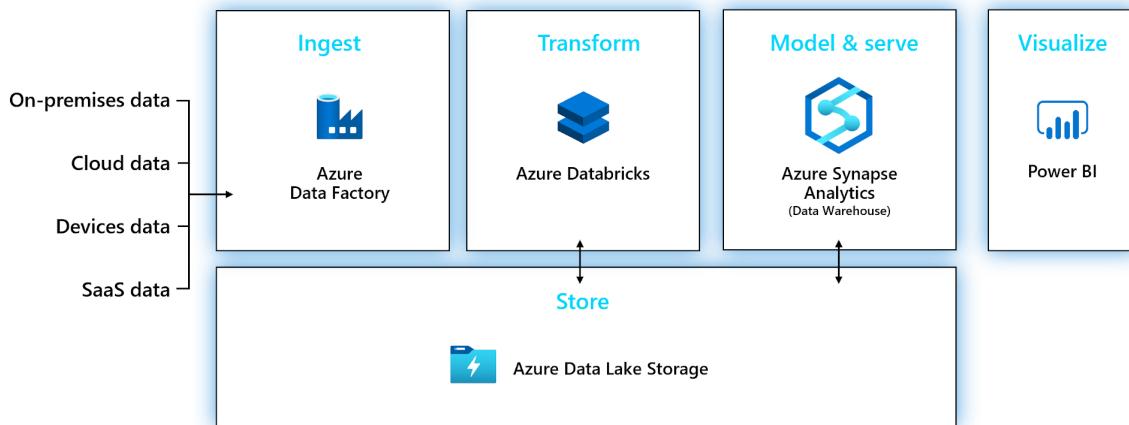
If the migration project includes any changes to the data model, the best practice is to perform these changes in the new target environment. That is, migrate the existing model first, and then use the power and flexibility of Azure Synapse Analytics to transform the data to the new model. This approach minimizes the impact on the existing system and uses the performance and scalability of Azure Synapse Analytics to make any changes quickly and cost-effectively.

You can migrate the existing system as several layers (for example, data ingest/staging layer, data warehouse layer, and reporting or data mart layer). Each layer consists of relational tables and views. Although you can migrate all these to Azure Synapse Analytics as is, it might be more cost-effective and reliable to use some of the features and capabilities of the Azure ecosystem. For example:

- **Data ingest and staging:** You can use Azure Blob storage in conjunction with PolyBase for fast parallel data loading for part of the ETL (extract, transform, load) or ELT (extract, load, transform) process, rather than relational tables.
- **Reporting layer and data marts:** The performance characteristics of Azure Synapse Analytics might eliminate the need to physically instantiate aggregated tables for reporting purposes or data marts. It might be possible to implement these as views onto the core data warehouse or via a third-party data

virtualization layer. At the basic level, you can achieve the process for data migration of historical data and possibly also incremental updates as shown in this diagram:

## Modern Data Warehouse



If you can use these or similar approaches, the number of tables to be migrated is reduced. Some processes might be simplified or eliminated, again reducing the migration workload. The applicability of these approaches depends on the individual use case. But the general principle is to consider using the features and facilities of the Azure ecosystem, where possible, to reduce the migration workload and build a cost-effective target environment. This also holds true for other functions, such as backup/restore and workflow management and monitoring.

Products and services available from Microsoft partners can assist in data warehouse migration and in some cases automate parts of the process. If the existing system incorporates a third-party ETL product, it might already support Azure Synapse Analytics as a target environment. The existing ETL workflows can be redirected to the new target data warehouse.

### Data marts: Physical or virtual

It's a common practice for organizations with older data warehouse environments to create data marts that provide their departments or business functions with good ad hoc self-service query and report performance. A data mart typically consists of a subset of the data warehouse that contains aggregated versions of the original data. Its form, typically a dimensional data model, supports users to easily query the data and receive fast response times from user-friendly tools like Tableau, MicroStrategy, or Microsoft Power BI.

One use of data marts is to expose the data in a usable form, even if the underlying warehouse data model is something different (such as a data vault). This approach is also known as a three-tier model.

You can use separate data marts for individual business units within an organization to implement robust data security regimes. For example, you can allow user access to specific data marts relevant to them and eliminate, obfuscate, or anonymize sensitive data.

If these data marts are implemented as physical tables, they require additional storage resources to house them and additional processing to build and refresh them regularly. Physical tables show that the data in the mart is only as current as the last refresh operation, so they may not be suitable for highly volatile data dashboards.

With the advent of relatively cheap scalable massively parallel processing (MPP) architectures such as Azure Synapse Analytics and their inherent performance characteristics, you might be able to provide data mart functionality without having to instantiate the mart as a set of physical tables. You achieve this by effectively virtualizing the data marts through one of these methods:

- SQL views on the main data warehouse.

- A virtualization layer that uses features such as views in Azure Synapse Analytics or third-party virtualization products such as Denodo.

This approach simplifies or eliminates the need for additional storage and aggregation processing. It reduces the overall number of database objects to be migrated.

Another benefit of the data warehouse approach is the capacity to run operations such as joins and aggregations on large data volumes. For example, implementing the aggregation and join logic within a virtualization layer and displaying external reporting in a virtualized view push the robust processing required to create these views into the data warehouse.

The primary drivers for choosing to implement physical or virtual data mart implementation are:

- More agility. A virtual data mart is easier to change than physical tables and the associated ETL processes.
- Lower total cost of ownership because of fewer data stores and copies of data in a virtualized implementation.
- Elimination of ETL jobs to migrate and simplified data warehouse architecture in a virtualized environment.
- Performance. Historically, physical data marts have been more reliable. Virtualization products are now implementing intelligent caching techniques to mitigate this.

You can also use data virtualization to display data to users consistently during a migration project.

## Data mapping

### Key and integrity constraints in Azure Synapse Analytics

Primary key and foreign key constraints are not currently enforced within Azure Synapse Analytics. However, you can include the definition for `PRIMARY KEY` in the `CREATE TABLE` statement with the `NOT ENFORCED` clause. This means that third-party reporting products can use the metadata for the table to understand the keys within the data model and therefore generate the most efficient queries.

### Data type support in Azure Synapse Analytics

Some older database systems include support for data types that are not directly supported within Azure Synapse Analytics. You can handle these data types by using a supported data type to store the data as is or by transforming the data to a supported data type.

Here's an alphabetical list of supported data types:

- `bigint`
- `binary [ (n) ]`
- `bit`
- `char [ (n) ]`
- `date`
- `datetime`
- `datetime2 [ (n) ]`
- `datetimeoffset [ (n) ]`
- `decimal [ (precision [, scale ]) ]`
- `float [ (n) ]`
- `int`
- `money`
- `nchar [ (n) ]`
- `numeric [ (precision [, scale ]) ]`
- `nvarchar [ (n | MAX) ]`
- `real [ (n) ]`
- `smalldatetime`
- `smallint`

- `smallmoney`
- `time [ (n) ]`
- `tinyint`
- `uniqueidentifier`
- `varbinary [ (n | MAX) ]`
- `varchar [ (n | MAX) ]`

The following table lists common data types that are not currently supported, together with the recommended approach for storing them in Azure Synapse Analytics. For specific environments such as Teradata or Netezza, see the associated documents for more detailed information.

UNSUPPORTED DATA TYPE	WORKAROUND
<code>geometry</code>	<code>varbinary</code>
<code>geography</code>	<code>varbinary</code>
<code>hierarchyid</code>	<code>nvarchar(4000)</code>
<code>image</code>	<code>varbinary</code>
<code>text</code>	<code>varchar</code>
<code>ntext</code>	<code>nvarchar</code>
<code>sql_variant</code>	Split column into several strongly typed columns
<code>table</code>	Convert to temporary tables
<code>timestamp</code>	Rework code to use <code>datetime2</code> and the <code>CURRENT_TIMESTAMP</code> function
<code>xml</code>	<code>varchar</code>
User-defined type	Convert back to the native data type when possible

#### Potential data issues

Depending on the source environment, some issues can cause problems when you're migrating data:

- There can be subtle differences in the way that `NULL` data is handled in different database products. Examples include collation sequence and handling of empty character strings.
- `DATE`, `TIME`, `INTERVAL`, and `TIME ZONE` data and associated functions can vary widely from product to product.

Test these thoroughly to determine whether the desired results are achieved in the target environment. The migration exercise can uncover bugs or incorrect results that are currently part of the existing source system, and the migration process is a good opportunity to correct anomalies.

#### Best practices for defining columns in Azure Synapse Analytics

It's common for older systems to contain columns with inefficient data types. For example, you might find a field defined as `VARCHAR(20)` when the actual data values would fit into a `CHAR(5)` field. Or, you might find the use of `INTEGER` fields when all values would fit within a `SMALLINT` field. Insufficient data types can lead to inefficiencies in both storage and query performance, especially in large fact tables.

It's a good time to check and rationalize current data definitions during a migration exercise. You can automate these tasks by using SQL queries to find the maximum numeric value or character length within a data field and comparing the result to the data type.

In general, it's a good practice to minimize the total defined row length for a table. For the best query performance, you can use the smallest data type for each column, as described earlier. The recommended approach to load data from external tables in Azure Synapse Analytics is to use the PolyBase utility, which supports a maximum defined row length of 1 megabyte (MB). PolyBase won't load tables with rows longer than 1 MB, and you must use [bcp](#) instead.

For the most efficient join execution, define the columns on both sides of the join as the same data type. If the key of a dimension table is defined as `SMALLINT`, then the corresponding reference columns in fact tables using that dimension should also be defined as `SMALLINT`.

Avoid defining character fields with a large default size. If the maximum size of data within a field is 50 characters, use `VARCHAR(50)`. Similarly, don't use `NVARCHAR` if `VARCHAR` will suffice. `NVARCHAR` stores Unicode data to allow for different language character sets. `VARCHAR` stores ASCII data and takes less space.

## Summary of design recommendations

Don't migrate unnecessary objects or processes. Use built-in features and functions in the target Azure environment where appropriate to reduce the actual number of objects and processes to migrate. Consider using a virtualization layer to reduce or eliminate the number of physical data marts that you'll migrate and to push down processing into the data warehouse.

Automate wherever possible, and use metadata from system catalogs in the source system to generate DDLs for the target environment. If possible, also automate generating documents. Microsoft partners such as WhereScape can provide specialized tools and services to assist with automation.

Perform any required data model changes or data mapping optimizations on the target platform. You can make these changes more efficiently in Azure Synapse Analytics. This approach reduces the impact on source systems that might already be running close to full capacity.

## Performance options

This section describes the features available within Azure Synapse Analytics that you can use to improve performance for a data model.

### General approach

The platform's features run performance tuning on the database that will be migrated. Indexes, data partitioning, and data distribution are examples of such performance tuning. When you're preparing for migration, documenting the tuning can capture and reveal optimizations that you can apply in the Azure Synapse Analytics target environment.

For example, the presence of a non-unique index on a table can indicate that fields used in the index are used frequently for filtering, grouping, or joining. This will still be the case in the new environment, so keep it in mind when you're choosing which fields to index there. Migration recommendations for specific source platforms such as Teradata and Netezza are described in detail in separate documents.

Use the performance and scalability of the target Azure Synapse Analytics environment to experiment with different performance options like data distribution. Determine the best choice of alternative approaches (for example, replicated versus hash-distributed for a large dimension table). This doesn't mean that data must be reloaded from external sources. It's relatively quick and easy to test alternative approaches in Azure Synapse Analytics by creating copies of any table with different partitioning or distribution options via a `CREATE TABLE AS SELECT` statement.

Use the monitoring tools provided by the Azure environment to understand how queries are executed and where bottlenecks might be occurring. Tools are also available from third-party Microsoft partners to provide monitoring dashboards and automated resource management and alerting.

Each SQL operation in Azure Synapse Analytics and resource, such as memory or the CPU used by that query, is logged into system tables. A series of dynamic management views simplifies access to this information.

The following sections explain the key options within Azure SQL Data Warehouse for tuning query performance. Existing environments will contain information about potential optimization in the target environment.

## Temporary tables

Azure Synapse Analytics supports temporary tables that are visible only to the session in which they were created. They exist for the duration of a user session and are automatically dropped at the end of the session.

To create a temporary table, prefix the table name with the hash character (#). You can use all the usual indexing and distribution options with temporary tables, as described in the next section.

Temporary tables have some restrictions:

- Renaming them isn't allowed.
- Viewing or partitioning them isn't allowed.
- Changing permissions isn't allowed.

Temporary tables are commonly used within ETL/ELT processing, where transient intermediate results are used as part of a transformation process.

## Table distribution options

Azure Synapse Analytics is an MPP database system that achieves performance and scalability by running in parallel across multiple processing nodes.

The ideal processing scenario for running an SQL query in a multinode environment is to balance the workload and give all nodes an equal amount of data to process. This approach also allows you to minimize or eliminate the amount of data that has to be moved between nodes to satisfy the query.

It can be challenging to achieve the ideal scenario because there are often aggregations in typical analytics queries and multiple joins between several tables, as between fact and dimension tables.

One way to influence how queries are processed is to use the distribution options within Azure Synapse Analytics to specify where each table's individual data rows are stored. For example, assume that two large tables are joined on the data column, CUSTOMER\_ID. By distributing the two tables through the CUSTOMER\_ID columns whenever that join is performed, you can ensure that the data from each side of the join will already be co-located on the same processing node. This method eliminates the need to move data between nodes. The distribution specification for a table is defined in the CREATE TABLE statement.

The following sections describe the available distribution options and recommendations for when to use them. It's possible to change the distribution of a table after the initial load, if necessary: re-create the table with the new distribution by using the CREATE TABLE AS SELECT statement.

### Round robin

Round-robin table distribution is the default option and spreads the data evenly across the nodes in the system. This method is good for fast data loading and for data that's relatively low in volume and doesn't have an obvious candidate for hashing. It's frequently used for staging tables as part of an ETL or ELT process.

### Hashed

The system assigns the row to a hash bucket, a task based on a hashing algorithm applied to a user-defined key like CUSTOMER\_ID in the preceding example. The bucket is then assigned to a specific node, and all data rows hash-distributed on the same value end up on the same processing node.

This method is useful for large tables that are frequently joined or aggregated on a key. Other large tables to be joined should be hashed on the same key if possible. If there are multiple candidates for the hash key, choose the most frequently joined one.

The hash column shouldn't contain nulls and isn't typically a date because many queries filter on date. Hashing is typically more efficient if the key to hash is an integer value instead of `CHAR` or `VARCHAR`. Avoid choosing keys with a highly skewed range of values, like when a small number of key values represent a large percentage of the data rows.

#### **Replicated**

Choosing replicated as the distribution option for a table will cause a complete copy of that table to be replicated on each compute node for query processing purposes.

This approach is useful for relatively small tables (typically less than 2 GB compressed) that are relatively static and frequently joined to larger tables via an equi-join. These tables are often dimensional tables in a star schema.

## **Indexing**

Azure Synapse Analytics includes options for indexing data in large tables to reduce the resources and time required to retrieve records:

- Clustered columnstore index
- Clustered index
- Non-clustered index

A non-indexed option, `HEAP`, exists for tables that don't benefit from any of the index options. Using indexes is a trade-off between improved query times versus longer load times and usage of more storage space. Indexes often speed up `SELECT`, `UPDATE`, `DELETE`, and `MERGE` operations on large tables that affect a small percentage of the data rows, and they can minimize full table scans.

Indexes are automatically created when `UNIQUE` or `PRIMARY KEY` constraints are defined on columns.

#### **Clustered columnstore index**

Clustered columnstore index is the default indexing option within Azure Synapse Analytics. It provides the best compression and query performance for large tables. For smaller tables of fewer than 60 million rows, these indexes aren't efficient, so you should use the `HEAP` option. Similarly, a heap or a temporary table might be more efficient if the data in a table is transient and part of an ETL/ELT process.

#### **Clustered index**

If there's a requirement to regularly retrieve a single row or small number of rows from a large table based on a strong filter condition, a clustered index might be more efficient than a clustered columnstore index. Only one clustered index is allowed per table.

#### **Non-clustered index**

Non-clustered indexes are similar to clustered indexes in that they can speed up retrieval of single rows or a small number of rows based on a filter condition. Internally, non-clustered indexes are stored separately from the data, and multiple non-clustered indexes can be defined on a table. However, each additional index will require more storage and will reduce the throughput of data insert or loading.

#### **Heap**

Heap tables incur none of the overhead associated with the creation and maintenance of indexes at data load time. They can help to quickly load transient data during processes, including ELT processes. Caching can also assist when the data is read immediately afterward. Because clustered columnstore indexes are inefficient below 60 million rows, heap tables can also help to store tables with rows less than this amount.

## **Data partitioning**

In an enterprise data warehouse, fact tables can contain many billions of rows. Partitioning is a way to optimize the maintenance and querying of these tables by splitting them into separate parts to reduce the amount of data

processed when running queries. The partitioning specification for a table is defined in the `CREATE TABLE` statement.

You can use only one field per table for partitioning. It's frequently a date field because many queries are filtered by a date or date range. You can change the partitioning of a table after initial load, if necessary, by re-creating the table with the new distribution through the `CREATE TABLE AS SELECT` statement.

#### Partitioning for query optimization

If queries against a large fact table are frequently filtered by a certain data column, then partitioning on that column can significantly reduce the amount of data that needs to be processed to perform the queries. A common example is to use a date field to split the table into smaller groups. Each group contains data for a single day. When a query contains a `WHERE` clause that filters on the date, only partitions that match the date filter need to be accessed.

#### Partitioning for optimization of table maintenance

It's common in data warehouse environments to maintain a rolling window of detailed fact data. An example is sales transactions that go back five years. By partitioning on the sales date, the removal of old data beyond the rolling window becomes much more efficient. Dropping the oldest partition is quicker and uses fewer resources than deletions of all the individual rows.

### Statistics

When a query is submitted to Azure Synapse Analytics, it's first processed by the query optimizer. The optimizer determines the best internal methods to execute the query efficiently.

The optimizer compares the various query-execution plans that are available based on a cost-based algorithm. The accuracy of the cost estimates is dependent on the statistics available. It's a good practice to ensure that statistics are up to date.

In Azure Synapse Analytics, if the `AUTO_CREATE_STATISTICS` option is turned on, it will trigger an automatic update of statistics. You can also create or update statistics manually via the `CREATE STATISTICS` command.

Refresh statistics when the contents have changed substantially, such as in a daily update. This refresh can be incorporated into an ETL process.

All tables in the database should have statistics collected on at least one column. It ensures that basic information such as row count and table size is available to the optimizer. Other columns that should have statistics collected are columns specified in `JOIN`, `DISTINCT`, `ORDER BY`, and `GROUP BY` processing.

### Workload management

Azure Synapse Analytics incorporates comprehensive features for managing resource utilization across mixed workloads. Creating resource classes for different workload types, such as queries versus data load, helps you manage your workload. It sets limits on the number of queries that run concurrently and on the compute resources assigned to each query. There's a trade-off between memory and concurrency:

- Smaller resource classes reduce the maximum memory per query but increase concurrency.
- Larger resource classes increase the maximum memory per query but reduce concurrency.

### Performance recommendations

Use performance improvement methods like indexes or data distribution to gauge candidates for similar methods in the new target environment, but benchmark to confirm that they're necessary in Azure Synapse Analytics. Build `COLLECT STATISTICS` steps into ETL/ELT processes to ensure that statistics are up to date, or select to automatically create statistics.

Understand the tuning options available in Azure Synapse Analytics and the performance characteristics of associated utilities, such as PolyBase for fast parallel data loading. Use these options to build an efficient end-to-end implementation.

Use the flexibility, scalability, and performance of the Azure environment to implement any data model changes or performance tuning options in place. This effort will reduce the impact on existing source systems.

Understand the dynamic management views available in Azure Synapse Analytics. These views provide both system-wide resource utilization information and detailed execution information for individual queries.

Understand Azure resource classes and allocate them appropriately to ensure efficient management of mixed workloads and concurrency.

Consider using a virtualization layer as part of the Azure Synapse Analytics environment. It can shield changes in the warehouse implementation from business users and reporting tools.

Research partner-provided migration tools and services such as Qlik Replicate for Microsoft migrations, WhereScape, and Datometry. These services can automate parts of the migration process and reduce the elapsed time and risk involved in a migration project.

# High availability for Azure Synapse Analytics

11/9/2020 • 2 minutes to read • [Edit Online](#)

One of the key benefits of a modern cloud-based infrastructure such as Microsoft Azure is that features for high availability (HA) and disaster recovery (DR) are built in and simple to implement and customize. These facilities are often lower in cost than the equivalent functionality within an on-premises environment. Using these built-in functions also means that the backup and recovery mechanisms in the existing data warehouse don't need to be migrated.

The following sections describe the standard Azure Synapse Analytics features that address requirements for high availability and disaster recovery.

## High availability

Azure Synapse Analytics uses database snapshots to provide high availability of the warehouse. A data warehouse snapshot creates a restore point that can be used to recover or copy a data warehouse to a previous state. Because Azure Synapse Analytics is a distributed system, a data warehouse snapshot consists of many files that are located in Azure Storage. Snapshots capture incremental changes from the data stored in your data warehouse.

Azure Synapse Analytics automatically takes snapshots throughout the day to create restore points that are available for seven days. This retention period can't be changed. Azure Synapse Analytics supports an eight-hour recovery point objective (RPO). You can restore a data warehouse in the primary region from any one of the snapshots taken in the past seven days.

The service also supports user-defined restore points. Manually triggering snapshots can create restore points of a data warehouse before and after large modifications. This capability ensures that restore points are logically consistent. Logical consistency provides additional data protection against workload interruptions or user errors for quick recovery time.

## Disaster recovery

In addition to the snapshots described earlier, Azure Synapse Analytics performs a standard geo-backup once per day to a paired datacenter. The RPO for a geo-restore is 24 hours. You can restore the geo-backup to a server in any other region where Azure Synapse Analytics is supported. A geo-backup ensures that a data warehouse can be restored in case the restore points in the primary region are not available.

# Governance or compliance strategy

11/9/2020 • 4 minutes to read • [Edit Online](#)

When governance or compliance is required throughout a migration effort, you need to broaden your scope to account for these requirements. The following guidance expands the scope of the [Azure migration guide](#) to address different approaches to addressing governance or compliance requirements.

## General scope expansion

Prerequisite activities are affected the most when governance or compliance are required. Additional adjustments can also be required during assessment, migration, and optimization.

## Suggested prerequisites

Configuration of the base Azure environment can change significantly when you're integrating governance or compliance requirements. To understand how prerequisites change, it's important to understand the nature of the requirements. Prior to beginning any migration that requires governance or compliance, you should choose and implement an approach in the cloud environment. The following are a few high-level approaches commonly seen during migrations:

**Common governance approach:** For most organizations, the [Cloud Adoption Framework governance model](#) is a sufficient approach. It consists of a minimum viable product (MVP) implementation, followed by targeted iterations of governance maturity to address tangible risks identified in the adoption plan. This approach provides the minimum tooling needed to establish consistent governance, so the team can understand the tools. It then expands on those tools to address common governance concerns.

**International Organization for Standardization (ISO) 27001 compliance blueprints:** If your organization is required to adhere to ISO compliance standards, the [ISO 27001 Shared Services blueprint samples](#) can serve as a more effective MVP. The blueprint can produce richer governance constraints, earlier in the iterative process. The [ISO 27001 App Service Environment/SQL Database workload blueprint sample](#) expands on the Shared Services blueprint, to map controls and deploy a common architecture for an application environment.

**Cloud Adoption Framework enterprise-scale landing zone:** You might require a more robust governance starting point. If so, consider the [Cloud Adoption Framework enterprise-scale landing zone](#). The Cloud Adoption Framework enterprise-scale landing zone approach focuses on adoption teams who have a mid-term objective (within 24 months) to host more than 1,000 assets (applications, infrastructure, or data assets) in the cloud. The Cloud Adoption Framework enterprise-scale landing zone is the *de facto* choice for complex governance scenarios for these larger cloud adoption efforts.

## Partnership option to complete prerequisites

**Microsoft Services:** Microsoft Services provides solution offerings that can align to the Cloud Adoption Framework governance model, compliance blueprints, or Cloud Adoption Framework enterprise-scale landing zone options. This option helps you to ensure that you're using the most appropriate governance or compliance model. Use the [Secure Cloud Insights](#) solution to establish a data-driven picture of a customer deployment in Azure. This solution also validates the customer's Azure implementation maturity while identifying optimization of existing deployment architectures. Secure Cloud Insights also helps you reduce risk pertaining to governance security and availability. Based on customer insights, you should lead with the following approaches:

- **Cloud foundation:** Establish the customer's core Azure designs, patterns, and governance architecture with the [hybrid cloud foundation](#) solution. Map the customer's requirements to the most appropriate reference architecture. Implement a minimum viable product consisting of shared services and IaaS workloads.

- **Cloud modernization:** Use the [cloud modernization](#) solution as a comprehensive approach to move applications, data, and infrastructure to an enterprise-ready cloud. You can also optimize and modernize after cloud deployment.
- **Innovate with cloud:** Engage the customer through the [cloud center of excellence \(CCoE\)](#) solution. It implements an agile approach to capture business requirements, and to reuse deployment packages aligned with security, compliance, and service management policies. It also maintains the alignment of the Azure platform with operational procedures.

## Assess process changes

During assessment, you must make additional decisions to align to the required governance approach. The cloud governance team provides all members of the cloud adoption team with any policy statements, architectural guidance, or governance or compliance requirements prior to the assessment of a workload.

### Suggested action during the assessment process

Governance and compliance assessment requirements are too customer-specific to provide general guidance on the actual steps taken during assessment. The process should include tasks and time for aligning to compliance and governance requirements.

For a deeper understanding of governance, read the overview of the [Disciplines of Cloud Governance](#). This section of the Cloud Adoption Framework includes templates to document the policies, guidance, and requirements for each of the following sections:

- [Cost Management discipline](#)
- [Security Baseline discipline](#)
- [Resource Consistency discipline](#)
- [Identity Baseline discipline](#)
- [Deployment Acceleration discipline](#)

For information about developing governance guidance based on the Cloud Adoption Framework governance model, see [Implement a cloud governance strategy](#).

## Optimize and promote process changes

During the optimization and promotion processes, the cloud governance team should invest time to test and validate adherence to governance and compliance standards. Additionally, this step is a good time for the cloud governance team to curate templates that provide additional guidance for future projects, particularly in the Deployment Acceleration discipline.

### Suggested action during the optimize and promote process

During this process, the project plan should include time allocations for the cloud governance team to execute a compliance review, for each workload planned for production promotion.

## Next steps

Return to the checklist to reevaluate any additional scope requirements for the migration effort.

### [Migration best practices checklist](#)

# Cloud Adoption Framework migration model

11/9/2020 • 3 minutes to read • [Edit Online](#)

This section of the Cloud Adoption Framework explains the principles behind its migration model. Wherever possible, this content attempts to maintain a vendor-neutral position while guiding you through the processes and activities that can be applied to any cloud migration, regardless of your chosen cloud vendor.

## Understand migration motivations

Cloud migration is a portfolio management effort, cleverly disguised as a technical implementation. During the migration process, you will decide to move some assets, invest in others, and retire obsolete or unused assets. Some assets will be optimized, refactored, or replaced entirely as part of this process. Each of these decisions should align with the motivations behind your cloud migration. The most successful migrations also go a step further and align these decisions with desired business outcomes.

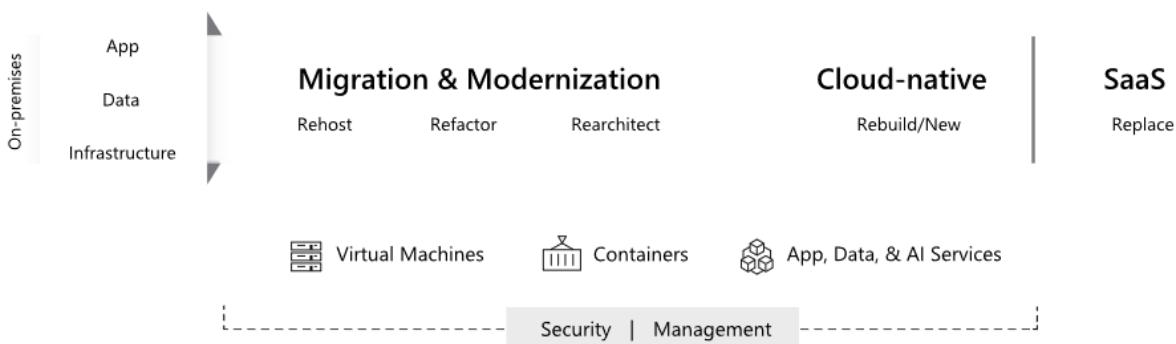
The Cloud Adoption Framework migration model depends on your organization having completed a process of business readiness for cloud adoption. Make sure you have reviewed the [Plan methodology](#) and the [Ready methodology](#) guidance in the Cloud Adoption Framework to determine the business drivers or other justification for a cloud migration, as well as any required organizational planning or training required before executing a migration process at scale.

### NOTE

While business planning is important, a growth mindset is equally important. In parallel with broader business planning efforts by the cloud strategy team, it's suggested that the cloud adoption team begin migrating a first workload as a precursor to wider scale migration efforts. This initial migration will allow the team to gain practical experience with the business and technical issues involved in a migration.

## Envision an end state

It's important to establish a rough vision of your end state before starting your migration efforts. The diagram below shows an on-premises starting point of infrastructure, applications, and data, which defines your *digital estate*. During the migration process, those assets are transitioned using one of the five migration strategies described in the [five Rs of rationalization](#).



Migration and modernization of workloads range from simple *rehost* migrations (also called *lift and shift* migrations) using infrastructure as a service (IaaS) capabilities that don't require code and application changes, through *refactoring* with minimal changes, to *rearchitecting* to modify and extend code and application functionality to take advantage of cloud technologies.

Cloud-native strategies and platform as a service (PaaS) strategies *rebuild* on-premises workloads using Azure

platform offerings and managed services. Workloads that have equivalent fully managed software as a service (SaaS) cloud-based offerings can often be fully *replaced* by these services as part of the migration process.

#### NOTE

During the public preview of the Cloud Adoption Framework, this section of the framework emphasizes a rehost migration strategy. Although PaaS and SaaS solutions are discussed as alternatives when appropriate, the migration of virtual machine-based workloads using IaaS capabilities is the primary focus.

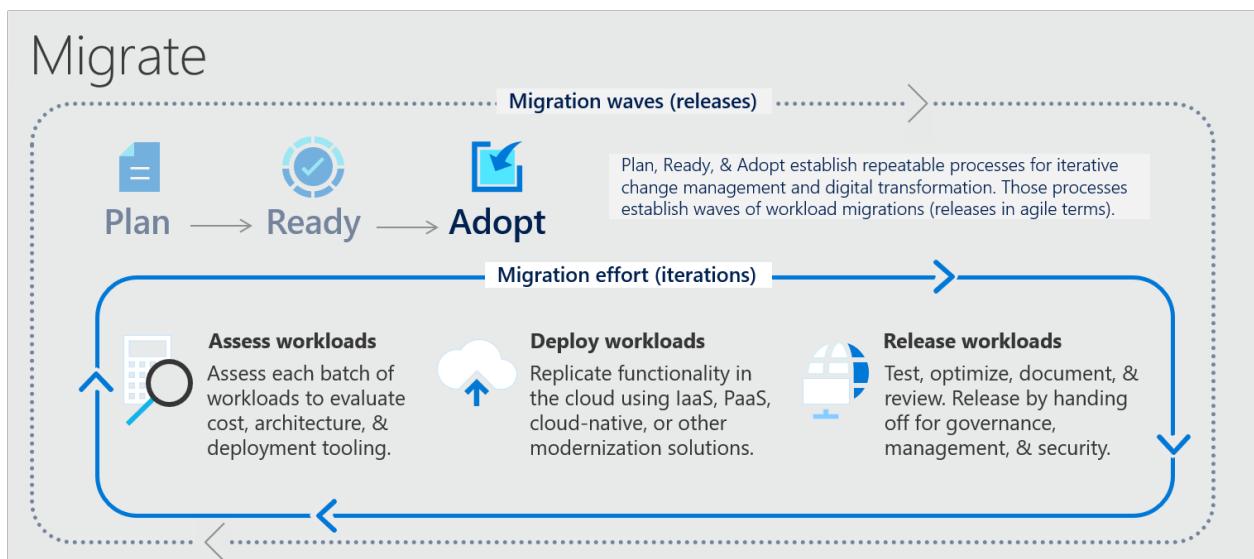
Other sections and future iterations of this content will expand on other approaches. For a high-level discussion on expanding the scope of your migration to include more complicated migration strategies, see the article [balancing the portfolio](#).

## Incremental migration

The Cloud Adoption Framework migration model is based on an incremental cloud transformation process. It assumes that your organization will start with an initial, limited-scope, cloud migration effort, which we refer to commonly as the first workload. This effort will expand iteratively to include more workloads as your operations teams refine and improve your migration processes.

Cloud migrations tools like [Azure Site Recovery](#) can migrate entire datacenters consisting of tens of thousands of VMs. However, the business and existing IT operations can seldom handle such a high pace of change. As such many organizations break up a migration effort into multiple iterations, moving one workload (or a collection of workloads) per iteration.

The principles behind this incremental model are based on the execution of processes and prerequisites referenced in the following infographic.



The consistent application of these principles represents an end goal for your cloud migration processes and should not be viewed as a required starting point. As your migration efforts mature, refer to the guidance in this section to help define the best process to support your organizational needs.

## Next steps

Begin learning about this model by [investigating the prerequisites to migration](#).

[Prerequisites to migration](#)

# Prerequisites for migration

11/9/2020 • 3 minutes to read • [Edit Online](#)

Prior to beginning any migrations, your migration target environment must be prepared for the coming changes. In this case, *environment* refers to the technical foundation in the cloud. Environment also means the business environment and mindset driving the migration. Likewise, the environment includes the culture of the teams executing the changes and those receiving the output. Lack of preparation for these changes is the most common reason for failure of migrations. This series of articles walks you through suggested prerequisites to prepare the environment.

## Objective

Ensure business, culture, and technical readiness prior to beginning an iterative migration plan.

## Review business drivers

Before beginning any cloud migration, review the [Plan methodology](#) and the [Ready methodology](#) in the Cloud Adoption Framework to ensure your organization is prepared for cloud adoption and migration processes. In particular, review the business requirements and expected outcomes driving the migration:

- [Get started: Accelerate migration](#)
- [Why are we moving to the cloud?](#)

## Definition of done

Prerequisites are completed when the following are true:

- **Business readiness.** The cloud strategy team has defined and prioritized a high-level migration backlog representing the portion of the digital estate to be migrated in the next two or three releases. The cloud strategy team and the cloud adoption team have agreed to an initial strategy for managing change.
- **Culture readiness.** The roles, responsibilities, and expectations of the cloud adoption team, cloud strategy team, and affected users have been agreed on regarding the workloads to be migrated in the next two or three releases.
- **Technical readiness.** The landing zone (or allocated hosting space in the cloud) that will receive the migrated assets meets minimum requirements to host the first migrated workload.

### Caution

Preparation is key to the success of a migration. However, too much preparation can lead to *analysis paralysis*, where too much time spent on planning can seriously delay a migration effort. The processes and prerequisites defined in this section are meant to help you make decisions, but don't let them block you from making meaningful progress.

Choose a relatively simple workload for your initial migration. Use the processes discussed in this section as you plan and implement this first migration. This first migration effort will quickly demonstrate cloud principles to your team and force them to learn about how the cloud works. As your team gains experience, integrate these learnings as you take on larger and more complex migrations.

## Accountability during prerequisites

Two teams are accountable for readiness during the prerequisites phase:

- **Cloud strategy team:** This team is responsible for identifying and prioritizing the first two or three workloads to serve as migration candidates.
- **Cloud adoption team:** This team is responsible for validating readiness of the technical environment and the feasibility of migrating the proposed workloads.

A single member of each team should be identified as accountable for each of the three definitions of done statements in the prior section.

## Responsibilities during prerequisites

In addition to the high-level accountability, there are actions that an individual or group needs to be directly responsible for. The following are a few such responsibilities that affect these activities:

- **Business prioritization.** Make business decisions regarding the workloads to be migrated and general timing constraints. For more information, see [Cloud migration business motivations](#).
- **Change management readiness.** Establish and communicate the plan for tracking technical change during migration.
- **Business user alignment.** Establish a plan for readying the business user community for migration execution.
- **Digital estate inventory and analysis.** Execution of the tools required to inventory and analyze the digital estate. See the Cloud Adoption Framework discussion of the [digital estate](#) for more information.
- **Cloud readiness.** Evaluate the target deployment environment to ensure that it complies with requirements of the first few workload candidates. See the [Azure setup guide](#) for more information.

The remaining articles in this series help with the execution of each.

## Next steps

With a general understanding of the prerequisites, you're ready to address the first prerequisite [early migration decisions](#).

[Early migration decisions](#)

# Decisions that affect migration

11/9/2020 • 6 minutes to read • [Edit Online](#)

During migration, several factors affect decisions and execution activities. This article explains the central theme of those decisions and explores a few questions that carry through the discussions of migration principles in this section of the Cloud Adoption Framework guidance.

## Business outcomes

The objective or goal of any adoption effort can have a significant impact on the suggested approach to execution.

- **Migration.** Urgent business drivers, speed of adoption, or cost savings are examples of operational outcomes. These outcomes are central to efforts that drive business value from transitive change in IT or operations models. The Migrate methodology of the Cloud Adoption Framework focuses heavily on migration focused business outcomes.
- **Application innovation.** Improving customer experience and growing market share are examples of incremental outcomes. The outcomes result from a collection of incremental changes focused on the needs and desires of current customers.
- **Data-driven innovation.** New products or services, especially ones that come from the power of data, are examples of disruptive outcomes. These outcomes are the result of experimentation and predictions that use data to disrupt status quo in the market.

No business would pursue just one of these outcomes. Without operations, there are no customers, and vice versa. Cloud adoption is no different. Companies commonly work to achieve each of these outcomes, but trying to focus on all of them simultaneously can spread your efforts too thin and slow progress on work that could most benefit your business needs.

This prerequisite isn't a demand for you to pick one of these three goals, but instead to help your cloud strategy team and your cloud adoption team establish a set of operational priorities that will guide execution for the next three to six months. These priorities are set by ranking each of the three itemized options from most significant to least significant, as they relate to the efforts this team can contribute to in the next one or two quarters.

### Act on migration outcomes

If operational outcomes rank highest in the list, this section of the Cloud Adoption Framework will suit your team well. In this section, it is assumed that you need to prioritize speed and cost savings as primary key performance indicators (KPIs), in which case a migration model to adoption would be well aligned with the outcomes. A migration-focused model is heavily predicated on lift and shift migration of infrastructure as a service (IaaS) assets to deplete a datacenter and to produce cost savings. In such a model, modernization may occur but is a secondary focus until the primary migration mission is realized.

### Act on application innovations

If market share and customer experience are your primary drivers, this section may not be the best section of the Cloud Adoption Framework to guide your teams' efforts. Application innovation requires a plan that focuses on the modernization and transition of workloads, regardless of the underlying infrastructure. In such a case, the guidance in this section can be informative but may not be the best approach to guide core decisions.

### Act on data innovations

If data, experimentation, research and development (R&D), or new products are your priority for the next six months or so, this section may not be the best section of the Cloud Adoption Framework to guide your teams' efforts. Any data innovation effort could benefit from guidance regarding the migration of existing source data.

However, the broader focus of that effort would be on the ingress and integration of additional data sources. Extending that guidance with predictions and new experiences is much more important than the migration of IaaS assets.

## Effort

Migration effort can vary widely depending on the size and complexities of the workloads involved. A smaller workload migration involving a few hundred virtual machines (VMs) is a tactical process, potentially being implemented using automated tools such as [Azure Migrate](#). Conversely, a large enterprise migration of tens of thousands of workloads requires a highly strategic process and can involve extensive refactoring, rebuilding, and replacing of existing applications integrating platform as a service (PaaS) and software as a service (SaaS) capabilities. [Identifying and balancing the scope](#) of your planned migrations is critical.

Before making any decisions that could have a long-term impact on the current migration program, it is vital that you create consensus on the following decisions.

### Effort type

In any migration of significant scale (more than 250 VMs), assets are migrated using a variety of transition options, discussed in the five Rs of rationalization: *rehost*, *refactor*, *rearchitect*, *rebuild*, and *replace*.

Some workloads are modernized through a *rebuild* or *rearchitect* process, creating more modern applications with new features and technical capabilities. Other assets go through a *refactor* process, for instance a move to containers or other more modern hosting and operational approaches that don't necessarily affect the solutions code base. Commonly, virtual machines and other assets that are more well established go through a *rehost* process, transitioning those assets from the datacenter to the cloud. Some workloads could potentially be migrated to the cloud, but instead should be *replaced* using service-based (SaaS-based) cloud services that meet the same business need—for example, by using Microsoft 365 as an alternative to migrating Exchange Server instances.

In the majority of scenarios, some business event creates a forcing function that causes a high percentage of assets to temporarily migrate using the *rehost* process, followed by a more significant secondary transition using one of the other migration strategies after they're in the cloud. This process is commonly known as a *cloud transition*.

During the process of [rationalizing the digital estate](#), these types of decisions are applied to each asset to migrate. However, the prerequisite needed at this time is to make a baseline assumption. Of the five migration strategies, which best aligns with the business objectives or business outcomes driving this migration effort? This decision serves as a guiding assumption throughout the migration effort.

### Effort scale

Scale of the migration is the next important prerequisite decision. The processes needed to migrate 1,000 assets are different from the processes required to move 10,000 assets. Before beginning any migration effort, it is important to answer the following questions:

- **How many assets support the migrating workloads today?** Assets include data structures, applications, VMs, and necessary IT appliances. Choose a relatively small workload for your first migration candidate.
- **Of those assets, how many are planned for migration?** It's common for some assets to be terminated during a migration process, due to lack of sustained end-user dependency.
- **What are the top-down estimates of the scale of migrateable assets?** For the workloads included for migration, estimate the number of supporting assets such as applications, virtual machines, data sources, and IT appliances. See the [digital estate](#) section of the Cloud Adoption Framework for guidance on identifying relevant assets.

### Effort timing

Often, migrations are driven by a compelling business event that is time sensitive. For instance, one common driver is the termination or renewal of a third-party hosting contract. Although there are many potential business events necessitating a migration, they share a common factor: an end date. It is important to understand the

timing of any approaching business events, so activities and velocity can be planned and validated properly.

## Recap

Before proceeding, document the following assumptions and share them with the cloud strategy team and the cloud adoption teams:

- Business outcomes.
- Roles, documented and refined for the *Assess, Migrate, Optimize, and Secure and manage* migration processes.
- Definition of done, documented and refined separately for these migration processes.
- Effort type.
- Effort scale.
- Effort timing.

## Next steps

After the process is understood among the team, it's time to review technical prerequisites. The [migration environment planning checklist](#) helps to ensure that the technical foundation is ready for migration.

Once the process is understood among the team, its time to review technical prerequisites the [migration planning checklist](#) will help ensure the technical foundation is ready for migration.

[Review the migration planning checklist](#)

# Migration environment planning checklist: Validate environmental readiness prior to migration

11/9/2020 • 3 minutes to read • [Edit Online](#)

As an initial step in the migration process, you need to create the right environment in the cloud to receive, host, and support migrating assets. This article provides a list of things to validate in the current environment prior to migration.

The following checklist aligns with the guidance in the [Ready methodology](#) of the Cloud Adoption Framework. Review that section for guidance regarding execution of any of the following.

## Effort type assumption

This article and checklist assume a *rehost* or *cloud transition* approach to cloud migration.

## Governance alignment

The first and most important decision regarding any migration-ready environment is the choice of governance alignment. Has a consensus been achieved regarding alignment of governance with the migration foundation? At a minimum, the cloud adoption team should understand whether this migration is landing in a single environment with limited governance, a fully governed environment factory, or some variant in between. For additional guidance on governance alignment, see the [Govern methodology](#).

## Operations management alignment

Before migrating assets into the cloud, it is important to understand any requirements or constraints regarding operations management. At a minimum, the migration environment should include any implementations required to meet the operations baseline. For additional guidance on operations alignment, see the [Manage methodology](#).

## Cloud readiness implementation

Whether you choose to align with a broader cloud governance strategy or not for your initial migration, you will need to ensure your cloud deployment environment is configured to support your workloads.

If you're planning to align your migration with a cloud governance strategy from the start, you'll need to apply the [Five Disciplines of Cloud Governance](#) to help inform decisions on policies, toolchains, and enforcement mechanisms that will align your cloud environment with overall corporate requirements. Consult the Cloud Adoption Framework [actionable governance design guides](#) for examples of how to implement this model using Azure services.

If your initial migrations are not closely aligned with a broader cloud governance strategy, the general issues of organization, access, and infrastructure planning still need to be managed. Consult the [Azure setup guide](#) for help with these cloud readiness decisions.

### Caution

We highly recommend that you develop a governance strategy for anything beyond your initial workload migration.

Regardless of your level of governance alignment, you will need to make decisions related to the following topics.

## **Resource organization**

Based on the governance alignment decision, an approach to the organization and deployment of resources should be established prior to migration.

## **Nomenclature**

A consistent approach for naming resources, along with consistent naming schemas, should be established prior to migration.

## **Resource governance**

A decision regarding the tools to govern resources should be made prior to migration. The tools do not need to be fully implemented, but a direction should be selected and tested. The cloud governance team should define and require the implementation of a minimum viable product (MVP) for governance tooling prior to migration.

# Network

Your cloud-based workloads will require the provisioning of virtual networks to support end-user and administrative access. Based on resource organization and resource governance decisions, you should select a network approach align it to IT security requirements. Further, your networking decisions should be aligned with any hybrid network constraints required to operate the workloads in the migration backlog and support any access to resources hosted on-premises.

# Identity

Cloud-based identity services are a prerequisite for offering identity and access management (IAM) for your cloud resources. Align your identity management strategy with your cloud adoption plans before proceeding. For example, when migrating existing on-premises assets, consider supporting a hybrid identity approach using [directory synchronization](#) to allow a consistent set of user credentials across your on-premises and cloud environments during and after the migration.

# Next steps

If the environment meets the minimum requirements, it may be deemed approved for migration readiness.

[Cultural complexity and change management](#) helps to align roles and responsibilities to ensure proper expectations during execution of the plan.

[Cultural complexity and change management](#)

# Prepare for cultural complexity: Aligning roles and responsibilities

11/9/2020 • 3 minutes to read • [Edit Online](#)

An understanding of the culture required to operate the existing datacenters is important to the success of any migration. In some organizations, datacenter management is contained within centralized IT operations teams. In these centralized teams, roles and responsibilities tend to be well defined and well understood throughout the team. For larger enterprises, especially those bound by third-party compliance requirements, the culture tends to be more nuanced and complex. Cultural complexity can lead to roadblocks that are difficult to understand and time consuming to overcome.

In either scenario, it's wise to invest in the documentation of roles and responsibilities required to complete a migration. This article outlines some of the roles and responsibilities seen in a datacenter migration, to serve as a template for documentation that can drive clarity throughout execution.

## Business functions

In any migration, there are a few key functions that are best executed by the business, whenever possible. Often, IT is capable of completing the following tasks. However, engaging members of the business could aid in reducing barriers later in the adoption process. It also ensures mutual investment from key stakeholders throughout the migration process.

PROCESS	ACTIVITY	DESCRIPTION
Assess	Business goals	Define the desired business outcomes of the migration effort.
Assess	Priorities	Ensure alignment with changing business priorities and market conditions.
Assess	Justification	Validate assumptions that drive changing business justifications.
Assess	Risk	Help the cloud adoption team understand the impact of tangible business risks.
Assess	Approve	Review and approve the business impact of proposed architecture changes.
Optimize	Change plan	Define a plan for consumption of change within the business, including periods of low activities and change freezes.
Optimize	Testing	Align power users capable of validating performance and functionality.

PROCESS	ACTIVITY	DESCRIPTION
Secure and manage	Interruption impact	Aid the cloud adoption team in quantifying the impact of a business process interruption.
Secure and manage	Service-level agreement (SLA) validation	Aid the cloud adoption team in defining service-level agreements and acceptable tolerances for business outages.

Ultimately, the cloud adoption team is accountable for each of these activities. However, establishing responsibilities and a regular cadence with the business for the completion of these activities on an established rhythm can improve stakeholder alignment and cohesiveness with the business.

## Common roles and responsibilities

Each process within the discussion of the Cloud Adoption Framework migration principles includes a process article outlining specific activities to align roles and responsibilities. For clarity during execution, a single accountable party should be assigned for each activity, along with any responsible parties required to support those activities. However, the following list contains a series of common roles and responsibilities that have a higher degree of impact on migration execution. These roles should be identified early in the migration effort.

### NOTE

In the following table, an accountable party should start the alignment of roles. That column should be customized to fit existing processes for efficient execution. Ideally, a single person should be assigned as the accountable party.

PROCESS	ACTIVITY	DESCRIPTION	ACCOUNTABLE PARTY
Prerequisite	Digital estate	Align the existing inventory to basic assumptions, based on business outcomes.	Cloud strategy team
Prerequisite	Migration backlog	Prioritize the sequence of workloads to be migrated.	Cloud strategy team
Assess	Architecture	Challenge initial assumptions to define the target architecture based on usage metrics.	Cloud adoption team
Assess	Approval	Approve the proposed architecture.	Cloud strategy team
Migrate	Replication access	Access to existing on-premises hosts and assets to establish replication processes.	Cloud adoption team
Optimize	Ready	Validate that the system meets performance and cost requirements prior to promotion.	Cloud adoption team

PROCESS	ACTIVITY	DESCRIPTION	ACCOUNTABLE PARTY
Optimize	Promote	Permissions to promote a workload to production and redirect production traffic.	Cloud adoption team
Secure and manage	Ops transition	Document production systems prior to production operations.	Cloud adoption team

**Caution**

For these activities, permissions and authorization heavily influence the accountable party, who must have direct access to production systems in the existing environment or must have means of securing access through other responsible actors. Determining this accountable party directly affects the promotion strategy during the migrate and optimize processes.

## Next steps

When the team has a general understanding of roles and responsibilities, it's time to begin preparing the technical details of the migration. Understanding [technical complexity and change management](#) can help prepare the cloud adoption team for the technical complexity of migration by aligning to an incremental change management process.

[Technical complexity and change management](#)

# Prepare for technical complexity: Agile change management

11/9/2020 • 12 minutes to read • [Edit Online](#)

When an entire datacenter can be deprovisioned and re-created with a single line of code, traditional processes struggle to keep up. The guidance throughout the Cloud Adoption Framework is built on practices like IT service management (ITSM), the open group architecture framework (TOGAF), and others. However, to ensure agility and responsiveness to business change, this framework molds those practices to fit agile methodologies and DevOps approaches.

When shifting to an agile model where flexibility and iteration are emphasized, technical complexity and change management are handled differently than they're in a traditional waterfall model focusing on a linear series of migration steps. This article outlines a high-level approach to change management in an agile-based migration effort. At the end of this article, you should have a general understanding of the levels of change management and documentation involved in an incremental migration approach. Additional training and decisions are required to select and implement agile practices based on that understanding. The intention of this article is to prepare cloud architects for a facilitated conversation with project management to explain the general concept of change management in this approach.

## Address technical complexity

When changing any technical system, complexity and interdependency inject risk into project plans. Cloud migrations are no exception. When moving thousands (or tens of thousands) of assets to the cloud, these risks are amplified. Detecting and mapping all dependencies across a large digital estate could take years. Few businesses can tolerate such a long analysis cycle. To balance the need for architectural analysis and business acceleration, the Cloud Adoption Framework focuses on an INVEST model for product backlog management. The following sections summarize this type of model.

## INVEST in workloads

The term *workload* appears throughout the Cloud Adoption Framework. A workload is a unit of application functionality that can be migrated to the cloud. It could be a single application, a layer of an application, or a collection of an application. The definition is flexible and may change at various phrases of migration. The Cloud Adoption Framework uses the term */INVEST* to define a workload.

INVEST is a common acronym in many agile methodologies for writing user stories or product backlog items, both of which are units of output in agile project management tools. The measurable unit of output in a migration is a migrated workload. The Cloud Adoption Framework modifies the INVEST acronym a bit to create a construct for defining workloads:

- **Independent:** A workload should not have any inaccessible dependencies. For a workload to be considered migrated, all dependencies should be accessible and included in the migration effort.
- **Negotiable:** As additional discovery is performed, the definition of a workload changes. The architects planning the migration could negotiate factors regarding dependencies. Examples of negotiation points could include prerelease of features, making features accessible over a hybrid network, or packaging all dependencies in a single release.
- **Valuable:** Value in a workload is measured by the ability to provide users with access to a production workload.
- **Estimable:** Dependencies, assets, migration time, performance, and cloud costs should all be estimable and

should be estimated prior to migration.

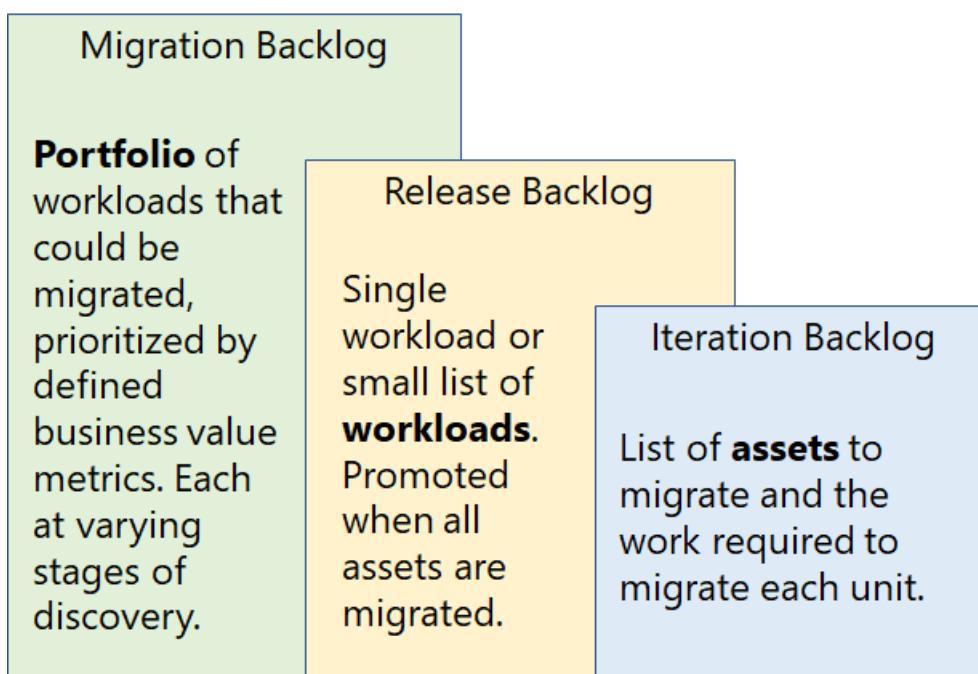
- **Small:** The goal is to package workloads in a single sprint. However, this may not always be feasible. Instead, teams are encouraged to plan sprints and releases to minimize the time required to move a workload to production.
- **Testable:** There should always be a defined means of testing or validating completion of the migration of a workload.

This acronym is not intended as a basis for rigid adherence but should help guide the definition of the term *workload*.

## Migration backlog: Aligning business priorities and timing

The migration backlog allows you to track your top-level portfolio of workloads that can be migrated. Prior to migration, the cloud strategy team and the cloud adoption team are encouraged to perform a review of the current [digital estate](#), and agree to a prioritized list of workloads to be migrated. This list forms the basis of the initial migration backlog.

Initially, workloads on the migration backlog are unlikely to meet the INVEST criteria outlined in the previous section. Instead, they serve as a logical grouping of assets from an initial inventory as a placeholder for future work. Those placeholders may not be technically accurate, but they serve as the basis for coordination with the business.



*The migration, release, and iteration backlogs track different levels of activity during migration processes.*

In any migration backlog, the change management team should strive to obtain the following information for any workload in the plan. At a minimum, this data should be available for any workloads prioritized for migration in the next two or three releases.

### Migration backlog data points

- **Business impact.** Understanding of the impact to the business of missing the expected timeline or reducing functionality during freeze windows.
- **Relative business priority.** A ranked list of workloads based on business priorities.
- **Business owner.** Document the one individual responsible for making business decisions regarding this workload.
- **Technical owner.** Document the one individual responsible for technical decisions related to this workload.
- **Expected timelines.** When the migration is scheduled for completion.

- **Workload freezes.** Time frames in which the workload should be ineligible for change.
- **Workload name.**
- **Initial inventory.** Any assets required to provide the functionality of the workload, including VMs, IT appliances, data, applications, deployment pipelines, and others. This information is likely to be inaccurate.

## Release backlog: Aligning business change and technical coordination

In the context of a migration, a *release* is an activity that deploys one or more workloads into production. A release generally covers several iterations or technical work. However, it represents a single iteration of business change. After one or more workloads have been prepared for production promotion, a release occurs. The decision to package a release is made when the workloads migrated represent enough business value to justify injecting change into a business environment. Releases are executed in conjunction with a [business change plan](#), after [business testing](#) has been completed. The cloud strategy team is responsible for planning and overseeing the execution of a release to ensure that the desired business change is released.

A *release backlog* is the future state plan that defines a coming release. Release backlog is the pivot point between business change management (*migration backlog*) and technical change management (*sprint backlog*). A release backlog consists of a list of workloads from the migration backlog that align to a specific subset of business outcome realization. Definition and submission of a release backlog to the cloud adoption team serve as a trigger for deeper analysis and migration planning. After the cloud adoption team has verified the technical details associated with a release, it can choose to commit to the release, establishing a release timeline based on current knowledge.

Given the degree of analysis required to validate a release, the cloud strategy team should maintain a running list of the next two to four releases. The team should also attempt to validate as much of the following information as possible, before defining and submitting a release. A disciplined cloud strategy team capable of maintaining the next four releases can significantly increase the consistency and accuracy of release timeline estimates.

### Release backlog data points

A partnership between the cloud strategy team and the cloud adoption team collaborates to add the following data points for any workloads in the release backlog:

- **Refined inventory.** Validation of required assets to be migrated. Often validated through log or monitoring data at the host, network, or OS level to ensure an accurate understanding of network and hardware dependencies of each asset under standard load.
- **Usage patterns.** An understanding of the patterns of usage from end users. These patterns often include an analysis of end-user geographical distribution, network routes, seasonal usage spikes, daily/hourly usage spikes, and end-user composition (interval versus external).
- **Performance expectations.** Analysis of available log data capturing throughput, page views, network routes, and other performance data required to replicate the end-user experience.
- **Dependencies.** Analysis of network traffic and application usage patterns to identify any additional workload dependencies, which should be factored into sequencing and environmental readiness. Don't include a workload in a release until one of the following criteria can be met:
  - All dependent workloads have been migrated.
  - Network and security configurations have been implemented to allow the workload to access all dependencies in alignment with existing performance expectations.
- **Desired migration approach.** At the migration backlog level, the assumed migration effort is the only consideration used in analysis. For instance, if the business outcome is an exit from an existing datacenter, all migrations are assumed to be a rehost scenario in the migration backlog. In the release backlog, the cloud strategy team and the cloud adoption team should evaluate the long-term value of additional features, modernization, and continued development investments to evaluate whether a more modern approach should be involved.
- **Business testing criteria.** After a workload is added to the migration backlog, testing criteria should be

mutually agreed on. In some cases, testing criteria can be limited to a performance test with a defined power user group. However, for statistical validation, an automated performance test is desired and should be included. The existing instance of the application often has no automated testing capabilities. Should this prove accurate, it is not uncommon for the cloud architects to work with power users to create a baseline load test against the existing solution to establish a benchmark to be used during migration.

### Release backlog cadence

In mature migrations, releases come in a regular cadence. The velocity of the cloud adoption team often normalizes, producing a release every two to four iterations (approximately every one or two months). However, this should be an organic outcome. Creating artificial release cadences can negatively affect the cloud adoption team's ability to achieve consistent throughput.

To stabilize business impact, the cloud strategy team should establish a monthly release process with the business to maintain regular dialogue but should also establish the expectation that it will be several months before a regular release cadence can be predicted.

## Sprint or iteration backlog: Aligning technical change and effort

A *sprint*, or *iteration*, is a consistent, time-bound unit of work. In the migration process, this is often measured in two-week increments. However, it's not unheard of to have one-week or four-week iterations. Creating time-bound iterations forces consistent intervals of effort completion and allows for more frequent adjustment to plans, based on new learnings. During any given sprint, there are usually tasks for the assessment, migration, and optimization of workloads defined in the migration backlog. Those units of work should be tracked and managed in the same project-management tool as the migration and release backlog, to drive consistency across each level of change management.

A *sprint backlog*, or *iteration backlog*, consists of the technical work to be completed in a single sprint or iteration, dealing with migrating individual assets. That work should be derived from the list of workloads being migrated. When using tools like Azure DevOps (previously Visual Studio online) for project management, the work items in a sprint would be children of the product backlog items in a release backlog and the epics in a migration backlog. Such a parent-child relationship allows for clarity at all levels of change management.

Within a single sprint or iteration, the cloud adoption team would work to deliver the committed amount of technical work, driving toward the migration of a defined workload. This is the end result of the change management strategy. When complete, these efforts can be tested by validating production readiness of a workload staged in the cloud.

### Large or complex sprint structures

For a small migration with a self-contained migration team, a single sprint could include all four phases of a migration for a single workload (*Assess*, *Migrate*, *Optimize*, and *Secure and manage*). More commonly, each of these processes shared by multiple teams in distinct work items across numerous sprints. Depending on the effort type, effort scale, and roles, these sprints can take a few different shapes.

- **Migration factory.** Large-scale migrations sometimes require an approach that resembles a factory in the execution model. In this model, various teams are allocated to the execution of a specific migration process (or subset of the process). After completion, the output of one team's sprint populates the backlog for the next team. This is an efficient approach for large-scale rehost migrations of many potential workloads involving thousands of virtual machines moving through phases of assessment, architecture, remediation, and migration. However, for this approach to work, a new homogenous environment with streamlined change management and approval processes is a must.
- **Migration waves.** Another approach that works well for large migrations is a wave model. In this model, division of labor isn't nearly as clear. Teams dedicate themselves to the migration process execution of individual workloads. However, the nature of each sprint changes. In one sprint, the team may complete assessment and architecture work. In another sprint, it may complete the migration work. In yet another sprint,

the focus would be on optimization and production release. This approach allows a core team to stay aligned to workloads, seeing them through the process in its entirety. When using this approach, the diversity of skills and context switching could reduce the potential velocity of the team, slowing the migration effort. Additionally, roadblocks during approval cycles can cause significant delays. It is important to maintain options in the release backlog to keep the team moving during blocked periods, with this model. It is also important to cross-train team members and to ensure that skill sets align with the theme of each sprint.

### Sprint backlog data points

The outcome of a sprint captures and documents the changes made to a workload, thus closing the change-management loop. When completed, at a minimum, the following should be documented. Throughout the execution of a sprint, this documentation should be completed in tandem with the technical work items.

- **Assets deployed.** Any assets deployed to the cloud to host the workload.
- **Remediation.** Any changes to the assets to prepare for cloud migration.
- **Configuration.** Chosen configuration of any assets deployed, including any references to configuration scripts.
- **Deployment model.** Approach used to deploy the asset to the cloud, including references to any deployment scripts or tools.
- **Architecture.** Documentation of the architecture deployed to the cloud.
- **Performance metrics.** Output of automated testing or business testing performed to validate performance at the time of deployment.
- **Unique requirements or configuration.** Any unique aspects of the deployment, configuration, or technical requirements necessary to operate the workload.
- **Operational approval.** Sign-off of validating operational readiness from the application owner and the IT operations staff responsible for managing the workload after deployment.
- **Architecture approval.** Sign-off from the workload owner and the cloud adoption team to validate any architecture changes required to host each asset.

## Next steps

After change management approaches have been established, it's time to address the final prerequisite, [migration backlog review](#)

[Migration backlog review](#)

# Migration backlog review

11/9/2020 • 2 minutes to read • [Edit Online](#)

The actionable output of the Plan phase is a migration backlog, which influences all of the prerequisites discussed so far. Development of the migration backlog should be completed as a first prerequisite. This article serves as a milestone to complete prerequisite activities. The cloud strategy team is accountable for the care and maintenance of the digital estate. However, the realization of the resultant backlog is the responsibility of every member of the migration effort. As a final prerequisite, the cloud strategy team and the cloud adoption team should review and understand the migration backlog. During that review, the members of both teams must gain sufficient knowledge to articulate the following key points in the migration backlog.

## Business outcomes and metrics

Every member of the team should understand the desired business outcomes. Migrations take time. It's easy for team members to become distracted by urgent but less important activities during migration. Establishing and reinforcing the desired outcomes helps the team understand the priority and relative importance of the migration, enabling better decision-making over time.

Tracking migration progress is equally important to the motivation of the team and to continued stakeholder support. Progress can be tracked through migration KPIs and learning metrics. Regardless of how the effort is tracked, it is important that the team is aware of these metrics so that they can evaluate performance during subsequent iterations.

## Business priorities

Sometimes, prioritizing one workload over another may seem illogical to the cloud adoption team. Understanding the business priorities that drove those decisions can help maintain the team's motivation. It also allows the team to make a stronger contribution to the prioritization process.

## Core assumptions

The article on [digital estate rationalization](#) discusses the agility and time-saving impact of basic assumptions when evaluating a digital estate. To fully realize those values, the cloud adoption team needs to understand the assumptions and the reasons that they were established. That knowledge better equips the cloud adoption team to challenge those assumptions.

## Next steps

With a general understanding of the digital estate and migration backlog, the team is ready to move beyond prerequisites and begin assessing workloads.

[Assess workloads](#)

# Assess workloads and validate assumptions before migration

11/9/2020 • 3 minutes to read • [Edit Online](#)

Many of your existing workloads are ideal candidates for cloud migration, but not every asset is compatible with cloud platforms and not all workloads can benefit from hosting in the cloud. [Digital estate planning](#) allows you to generate an overall [migration backlog](#) of potential workloads to migrate. However, this planning effort is high-level. It relies on assumptions made by the cloud strategy team and does not dig deeply into technical considerations.

As a result, before migrating a workload to the cloud it's critical to assess the individual assets associated with that workload for their migration suitability. During this assessment, your cloud adoption team should evaluate technical compatibility, required architecture, performance/sizing expectations, and dependencies to ensure that the migrated workload can be deployed to the cloud effectively.

The *assess* process is the first of four incremental activities that occur within an iteration. As discussed in the prerequisite article regarding [technical complexity and change management](#), a decision should be made in advance to determine how this phase is executed. In particular, will assessments be completed by the cloud adoption team during the same sprint as the actual migration effort? Alternatively, will a wave or factory model be used to complete assessments in a separate iteration? If the answer to this basic process question can't be answered by every member of the team, it may be wise to revisit the [prerequisites](#) section.

## Objective

Assess a migration candidate, evaluating the workload, associated assets, and dependencies prior to migration.

## Definition of done

This process is complete when the following are known about a single migration candidate:

- The path from on-premises to cloud, including production promotion approach decision, has been defined.
- Any required approvals, changes, cost estimates, or validation processes have been completed to allow the cloud adoption team to execute the migration.

## Accountability during assessment

The cloud adoption team is accountable for the entire assessment process. However, members of the cloud strategy team has a few responsibilities, as listed in the following section.

## Responsibilities during assessment

In addition to the high-level accountability, there are actions that an individual or group needs to be directly responsible for. The following are a few activities that require assignments to responsible parties:

- **Business priority.** The team understands the purpose for migrating this workload, including any intended impact to the business.
  - A member of the cloud strategy team should carry final responsibility for this activity, under the direction of the cloud adoption team.
- **Stakeholder alignment.** The team aligns expectations and priorities with internal stakeholders, identifying success criteria for the migration. What does success look like post-migration?

- **Refined rationalization.** Evaluate the initial assumptions regarding rationalization. Should a different [rationalization approach](#) be used to migrate this specific workload?
- **Modernization decisions.** Regardless of the rationalization decision, should various assets in the workload be modernized to use PaaS-based solutions?
- **Cost.** The cost of the target architecture has been estimated, and the overall budget has been adjusted.
- **Migration support.** The team has decided how the technical work of the migration will be completed, including decisions regarding partner or Microsoft support.
- **Evaluation.** The workload is evaluated for compatibility and dependencies.
  - This activity should be assigned to a subject matter expert who is familiar with the architecture and operations of the candidate workload.
- **Architect.** The team has agreed on the final state architecture for the migrated workload.
- **Migration tooling.** Depending on modernization and architecture approaches, a variety of migration tools could be used to automate the migration. Based on the proposed architecture, will this migration use the best [migration tools](#)?
- **Backlog alignment.** The cloud adoption team reviews requirements and commits to the migration of the candidate workload. After commitment, the release backlog and iteration backlog are to be updated accordingly.
- **Work breakdown structure or work-back schedule.** The team establishes a schedule of major milestones identifying goals for when planning, implementation, and review processes are completed.
- **Final approval.** Any necessary approvers have reviewed the plan and have signed off on the approach to migrate the asset.
  - To avoid surprises later in the process, at least one representative of the business should be involved in the approval process.

**Caution**

This full list of responsibilities and actions can support large and complex migrations involving multiple roles with varying levels of responsibility, and requiring a detailed approval process. Smaller and simpler migration efforts may not require all of roles and actions described here. To determine which of these activities add value and which are unnecessary, your cloud adoption team and the cloud strategy team should use this complete process as part of your first workload migration. After the workload has been verified and tested, the team can evaluate this process and choose which actions to use moving forward.

## Next steps

With a general understanding of the assessment process, you're ready to begin the process by [classifying workloads](#).

[Classify workloads](#)

# Workload classification before migration

11/9/2020 • 2 minutes to read • [Edit Online](#)

During each iteration of any migration process, one or more workloads will be migrated and promoted to production. Prior to either of those migration activities, it is important to classify each workload. Classification helps clarify governance, security, operations, and data management requirements.

The following guidance builds on the suggested tagging requirements outlined in the [naming and tagging standards article](#) by adding important [operations](#) and [governance](#) elements.

In this article, we specifically suggest adding criticality and data sensitivity to your existing tagging standards. Each of these data points will help other teams understand which workloads may require additional attention or support.

## Data sensitivity

As outlined in the article on [data classification](#), data classification measures the impact that a data leak would have on the business or customers. The governance and security teams use data sensitivity or data classification as an indicator of security risks. During assessment, the cloud adoption team should evaluate the data classification for each workload targeted for migration and share that classification with supporting teams. Workloads that deal strictly in "public data" may not have any impact on supporting teams. However, as data moves further towards the "highly confidential" end of the spectrum, both governance and security teams will likely have a vested interest in participating in the assessment of the workload.

Work with your security and governance teams as early as possible to define the following items:

- A clear process for sharing any workloads on the backlog with sensitive data.
- An understanding of the governance requirements and security baseline required for various different levels of data sensitivity.
- Any impact data sensitivity may have on subscription design, management group hierarchies, or landing zone requirements.
- Any requirements for testing data classification, which may include specific tooling or defined scope of classification.

## Mission criticality

As outlined in the article on [workload criticality](#), the criticality of a workload is a measure of how significantly the business will be affected during an outage. This data point helps operations management and security teams evaluate risks regarding outages and breaches. During assessment, the cloud adoption team should evaluate mission criticality for each workload targeted for migration and share that classification with supporting teams. "Low" or "unsupported" workloads are likely to have little impact on the supporting teams. However, as workloads approach "mission critical" or "unit critical" classifications, their operational dependencies become more apparent.

Work with your security and operations teams as early as possible to define the following items:

- A clear process for sharing any workloads on the backlog with support requirements.
- An understanding of the operations management and resource consistency requirements for various different levels of criticality.
- Any impact criticality may have on subscription design, management group hierarchies, or landing zone requirements.
- Any requirements for documenting criticality, which might include specific traffic or usage reports, financial

analyses, or other tools.

## Next steps

Once workloads are properly classified, it's much easier to [align business priorities](#).

[Align business priorities](#)

# Business priorities: Maintaining alignment

11/9/2020 • 3 minutes to read • [Edit Online](#)

*Transformation* is often defined as a dramatic or spontaneous change. At the board level, change can look like a dramatic transformation. However, for those who work through the process of change in an organization, transformation is a bit misleading. Under the surface, transformation is better described as a series of properly executed transitions from one state to another.

The amount of time required to rationalize or transition a workload will vary, depending on the technical complexity involved. However, even when this process can be applied to a single workload or group of applications quickly, it takes time to produce substantial changes among a user base. It takes longer for changes to propagate through various layers of existing business processes. If transformation is expected to shape behavior patterns in consumers, the results can take longer to produce significant results.

Unfortunately, the market doesn't wait for businesses to transition. Consumer behavior patterns change on their own, often unexpectedly. The market's perception of a company and its products can be swayed by social media or a competitor's positioning. Fast and unexpected market changes require companies to be nimble and responsive.

The ability to execute processes and technical transitions requires a consistent, stable effort. Quick decisions and nimble actions are needed to respond to market conditions. These two are at odds, making it easy for priorities to fall out of alignment. This article describes approaches to maintaining transitional alignment during migration efforts.

## How can business and technical priorities stay aligned during a migration?

The cloud adoption team and the cloud governance team focus on the execution of the current iteration and current release. Iterations provide stable increments of technical work, thus avoiding costly disruptions that would otherwise slow the progress of migration efforts. Releases ensure that the technical effort and energy stay focused on the business objectives of the workload migration. A migration project could require many releases over an extended period. By the time it is completed, market conditions have likely changed significantly.

In parallel, the cloud strategy team focuses on executing the business change plan and preparing for the next release. The cloud strategy team generally looks at least one release ahead, and it monitors for changing market conditions and adjusts the migration backlog accordingly. This focus of managing transformation and adjusting the plan creates natural pivots around the technical work. When business priorities change, adoption is only one release behind, creating technical and business agility.

## Business alignment questions

The following questions can help the cloud strategy team shape and prioritize the migration backlog to help ensure that the transformation effort best aligns with current business needs.

- Has the cloud adoption team identified a list of workloads ready for migration?
- Has the cloud adoption team selected a single candidate for an initial migration from that list of workloads?
- Do the cloud adoption team and the cloud governance team have all of the necessary data regarding the workload and cloud environment to be successful?
- Does the candidate workload deliver the most relevant impact for the business in the next release?
- Are there other workloads that are better candidates for migration?

## Tangible actions

During the execution of the business change plan, the cloud strategy team monitors for positive and negative results. When those observations require technical change, the adjustments are added as work items to the release backlog to be prioritized in the next iteration.

When the market changes, the cloud strategy team works with the business to understand how to best respond to the changes. When that response requires a change in migration priorities, the migration backlog is adjusted. This moves up workloads that were previously lower in priority.

## Next steps

With properly aligned business priorities, the cloud adoption team can confidently begin to [evaluate workloads](#) to develop architecture and migration plans.

[Evaluate workloads](#)

# Evaluate workload readiness

11/9/2020 • 3 minutes to read • [Edit Online](#)

This activity focuses on evaluating readiness of a workload to migrate to the cloud. During this activity, the cloud adoption team validates that all assets and associated dependencies are compatible with the chosen deployment model and cloud provider. During the process, the team documents any efforts required to [remediate compatibility issues](#).

## Evaluation assumptions

Most of the content discussing principles in the Cloud Adoption Framework is cloud agnostic. However, the readiness evaluation process must be largely specific to each specific cloud platform. The following guidance assumes an intention to migrate to Azure. It also assumes use of Azure Migrate (also known as Azure Site Recovery) for [replication activities](#). For alternative tools, see [Replication options](#).

This article doesn't capture all possible evaluation activities. It is assumed that each environment and business outcome will dictate specific requirements. To help accelerate the creation of those requirements, the remainder of this article shares a few common evaluation activities related to [infrastructure](#), [database](#), and [network](#) evaluation.

## Common infrastructure evaluation activities

- VMware requirements: review the [Azure Site Recovery requirements for VMware](#).
- Hyper-V requirements: review the [Azure Site Recovery requirements for Hyper-V](#).

Be sure to document any discrepancies in host configuration, replicated VM configuration, storage requirements, or network configuration.

## Common database evaluation activities

- Document the recovery point objectives (RPOs) and recovery time objectives (RTOs) of the current database deployment. These are used during [architecture activities](#) to aid in decision-making.
- Document any requirements for high-availability configuration. For assistance understanding SQL Server requirements, see the [SQL Server high availability solutions guide](#).
- Evaluate PaaS compatibility. The [Azure data migration guide](#) maps on-premises databases to compatible Azure PaaS solutions, like [Azure Cosmos DB](#), [Azure SQL Database](#) [Azure Database for MySQL](#), [Azure Database for PostgreSQL](#), or [Azure Database for MariaDB](#).
- When PaaS compatibility is an option without the need for any remediation, consult the team responsible for [architecture activities](#). PaaS migrations can produce significant time savings and reductions in the total cost of ownership (TCO) of most cloud solutions.
- When PaaS compatibility is an option but remediation is required, consult the teams responsible for [architecture activities](#) and [remediation activities](#). In many scenarios, the advantages of PaaS migrations for database solutions can outweigh the increase in remediation time.
- Document the size and rate of change for each database to be migrated.
- When possible, document any applications or other assets that make calls to each database.

**NOTE**

Synchronization of any asset consumes bandwidth during the replication processes. A very common pitfall is to overlook the bandwidth consumption required to keep assets synchronized between the point of replication and release. Databases are common consumers of bandwidth during release cycles, and databases with large storage footprints or a high rate of change are especially concerning. Consider an approach of replicating the data structure, with controlled updates before user acceptance testing (UAT) and release. In such scenarios, alternatives to Azure Site Recovery may be more appropriate. For more information, see guidance from the [Azure Database Migration Guide](#).

## Common network evaluation activities

- Calculate the total storage for all VMs to be replicated during the iterations leading up to a release.
- Calculate the drift or change rate of storage for all VMs to be replicated during the iterations leading up to a release.
- Calculate the bandwidth requirements needed for each iteration by summing total storage and drift.
- Calculate unused bandwidth available on the current network to validate per iteration alignment.
- Document bandwidth needed to reach anticipated migration velocity. If any remediation is required to provide necessary bandwidth, notify the team responsible for [remediation activities](#).

**NOTE**

Total storage directly affects bandwidth requirements during initial replication. However, storage drift continues from the point of replication until release. This means that drift has a cumulative effect on available bandwidth.

## Next steps

After the evaluation of a system is complete, the outputs feed the development of a new [cloud architecture](#).

[Architect workloads prior to migration](#)

# Architect workloads prior to migration

3/31/2020 • 3 minutes to read • [Edit Online](#)

This article expands on the assessment process by reviewing activities associated with defining the architecture of a workload within a given iteration. As discussed in the article on [incremental rationalization](#), some architectural assumptions are made during any business transformation that requires a migration. This article clarifies those assumptions, shares a few roadblocks that can be avoided, and identifies opportunities to accelerate business value by challenging those assumptions. This incremental model for architecture allows teams to move faster and to obtain business outcomes sooner.

## Architecture assumptions prior to migration

The following assumptions are typical for any migration effort:

- **IaaS.** It is commonly assumed that migrating workloads primarily involves the movement of virtual machines from a physical datacenter to a cloud datacenter via an IaaS migration, requiring a minimum of redevelopment or reconfiguration. This is known as a *lift and shift* migration. (Exceptions follow.)
- **Architecture consistency.** Changes to core architecture during a migration considerably increase complexity. Debugging a changed system on a new platform introduces many variables that can be difficult to isolate. For this reason, workloads should undergo only minor changes during migration and any changes should be thoroughly tested.
- **Retirement test.** Migrations and the hosting of assets consume operational and potential capital expenses. It is assumed that any workloads being migrated have been reviewed to validate ongoing usage. The choice to retire unused assets produces immediate cost savings.
- **Resize assets.** It is assumed that few on-premises assets are fully using the allocated resources. Prior to migration, it is assumed that assets will be resized to best fit actual usage requirements.
- **Business continuity and disaster recovery (BCDR) requirements.** It is assumed that an agreed-on SLA for the workload has been negotiated with the business prior to release planning. These requirements are likely to produce minor architecture changes.
- **Migration downtime.** Likewise, downtime to promote the workload to production can have an adverse effect on the business. Sometimes, the solutions that must transition with minimum downtime need architecture changes. It is assumed that a general understanding of downtime requirements has been established prior to release planning.

## Roadblocks that can be avoided

The itemized assumptions can create roadblocks that could slow progress or cause later pain points. The following are a few roadblocks to watch for, prior to the release:

- **Paying for technical debt.** Some aging workloads carry with them a high amount of technical debt. This can lead to long-term challenges by increasing hosting costs with any cloud provider. When technical debt unnaturally increases hosting costs, alternative architectures should be evaluated.
- **User traffic patterns.** Existing solutions may depend on existing network routing patterns. These patterns could slow performance considerably. Further, introduction of new hybrid wide area network (WAN) solutions can take weeks or even months. Prepare early in the architecture process for these roadblocks by considering traffic patterns and changes to any core infrastructure services.

## Accelerate business value

Some scenarios could require an different architecture than the assumed IaaS rehosting strategy. The following are a few examples:

- PaaS alternatives. PaaS deployments can reduce hosting costs, and they can also reduce the time required to migrate certain workloads. For a list of approaches that could benefit from a PaaS conversion, see the article on [evaluating assets](#).
- Scripted deployments/DevOps. If a workload has an existing DevOps deployment or other forms of scripted deployment, the cost of changing those scripts could be lower than the cost of migrating the asset.
- Remediation efforts. The remediation efforts required to prepare a workload for migration can be extensive. In some cases, it makes more sense to modernize the solution than it does to remediate underlying compatibility issues.

In each of these itemized scenarios, an alternative architecture could be the best possible solution.

## Next steps

After the new architecture is defined, [accurate cost estimations can be calculated](#).

[Estimate cloud costs](#)

# Estimate cloud costs

11/9/2020 • 2 minutes to read • [Edit Online](#)

During migration, there are several factors that can affect decisions and execution activities. To help understand which of those options are best for different situations, this article discusses various options for estimating cloud costs.

## Digital estate size

The size of your digital estate directly affects migration decisions. Migrations that involve fewer than 250 VMs can be estimated much more easily than a migration involving 10,000+ VMs. It's highly recommended that you select a smaller workload as your first migration. This gives your team a chance to learn how to estimate the costs of a simple migration effort before attempting to estimate larger and more complicated workload migrations.

However, note that smaller, single-workload, migrations can still involve a widely varying amount of supporting assets. If your migration involves under 1,000 VMs, a tool like [Azure Migrate](#) is likely sufficient to gather data on the inventory and forecast costs. Additional cost-estimate tooling options are described in the article on [digital estate cost calculations](#).

For 1,000+ unit digital estates, it's still possible to break down an estimate into four or five actionable iterations, making the estimation process manageable. For larger estates or when a higher degree of forecast accuracy is required, a more comprehensive approach, like that outlined in the [digital estate](#) section of the Cloud Adoption Framework, will likely be required.

## Accounting models

### Accounting models

If you're familiar with traditional IT procurement processes, estimation in the cloud may seem foreign. When adopting cloud technologies, acquisition shifts from a rigid, structured capital expense model to a fluid operating expense model. In the traditional capital expense model, the IT team would attempt to consolidate buying power for multiple workloads across various programs to centralize a pool of shared IT assets that could support each of those solutions. In the operating expenses cloud model, costs can be directly attributed to the support needs of individual workloads, teams, or business units. This approach allows for a more direct attribution of costs to the supported internal customer. When estimating costs, it's important to first understand how much of this new accounting capability will be used by the IT team.

For those wanting to replicate the legacy capital expense approach to accounting, use the outputs of either approach suggested in the [digital estate size](#) section above to get an annual cost basis. Next, multiply that annual cost by the company's typical hardware refresh cycle. Hardware refresh cycle is the rate at which a company replaces aging hardware, typically measured in years. Annual run rate multiplied by hardware refresh cycle creates a cost structure similar to a capital expense investment pattern.

## Next steps

After estimating costs, migration can begin. However, it would be wise to review partnership and support options before beginning any migration.

[Understand partnership and support options](#)

# Understand partnership and support options

11/9/2020 • 5 minutes to read • [Edit Online](#)

During migration, the cloud adoption team performs the actual migration of workloads to the cloud. Unlike the collaborative and problem-solving tasks when defining the [digital estate](#) or building the core cloud infrastructure, migration tends to be a series of repetitive execution tasks. Beyond the repetitive aspects, there are likely testing and tuning efforts that require deep knowledge of the chosen cloud provider. The repetitive nature of this process can sometimes be best addressed by a partner, reducing strain on full-time staff. Additionally, partners may be able to better align deep technical expertise when the repetitive processes encounter execution anomalies.

Partners tend to be closely aligned with a single cloud vendor or a small number of cloud vendors. To better illustrate partnership options, the remainder of this article assumes that Microsoft Azure is the chosen cloud provider.

During plan, build, or migrate, a company generally has four execution partnership options:

- **Guided self-service.** The existing technical team executes the migration, with help from Microsoft.
- **FastTrack for Azure.** Use the Microsoft FastTrack for Azure program to accelerate migration.
- **Solutions partner.** Get connected with Azure partners or cloud solution providers (CSPs) to accelerate migration.
- **Supported self-service.** Execution is completed by the existing technical staff with support from Microsoft.

## Guided self-service

If an organization is planning an Azure migration on its own, Microsoft is always there to assist throughout the journey. To help fast-track migration to Azure, Microsoft and its partners have developed an extensive set of architectures, guides, tools, and services to reduce risk and to speed migration of virtual machines, applications, and databases. These tools and services support a broad selection of operating systems, programming languages, frameworks, and databases.

- **Assessment and migration tools.** Azure provides a wide range of tools to be used in different phases for your cloud transformation, including assessing your existing infrastructure. For more information, refer to the "assess" section in the "migration" chapter that follows.
- **Microsoft Cloud Adoption Framework.** This framework presents a structured approach to cloud adoption and migration. It is based on best practices across many Microsoft-supported customer engagements and is organized as a series of steps, from architecture and design to implementation. For each step, supporting guidance helps you with the design of your application architecture.
- **Cloud design patterns.** Azure provides some useful cloud design patterns for building reliable, scalable, secure workloads in the cloud. Each pattern describes the problem that the pattern addresses, considerations for applying the pattern, and an example based on Azure. Most of the patterns include code samples or snippets that show how to implement the pattern on Azure. However, they're relevant to any distributed system, whether hosted on Azure or on other cloud platforms.
- **Cloud fundamentals.** Fundamentals help teach the basic approaches to implementation of core concepts. This guide helps technicians think about solutions that go beyond a single Azure service.
- **Example scenarios.** The guide provides references from real customer implementations, outlining the tools, approaches, and processes that past customers have followed to accomplish specific business goals.
- **Reference architectures.** Reference architectures are arranged by scenario, with related architectures grouped together. Each architecture includes best practices, along with considerations for scalability, availability, manageability, and security. Most also include a deployable solution.

## FastTrack for Azure

[FastTrack for Azure](#) provides direct assistance from Azure engineers, working hand in hand with partners, to help customers build Azure solutions quickly and confidently. FastTrack brings best practices and tools from real customer experiences to guide customers from setup, configuration, and development to production of Azure solutions, including:

- Datacenter migration
- Windows Server on Azure
- Linux on Azure
- SAP on Azure
- Business continuity and disaster recovery (BCDR)
- High-performance computing
- Cloud-native applications
- DevOps
- Application modernization
- Cloud-scale analytics
- Intelligent applications
- Intelligent agents
- Data modernization to Azure
- Security and management
- Globally distributed data
- Windows Virtual Desktop
- Azure Marketplace
- Fundamentals and governance

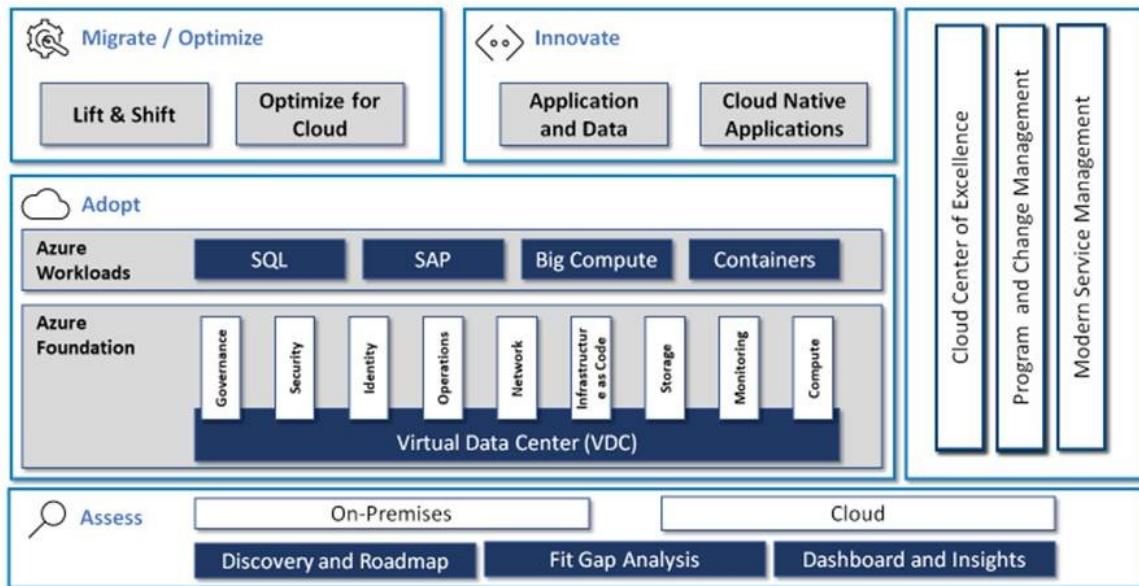
During a typical FastTrack for Azure engagement, Microsoft helps to define the business vision to plan and develop Azure solutions successfully. The team assesses architectural needs and provides guidance, design principles, tools, and resources to help build, deploy, and manage Azure solutions. The team matches skilled partners for deployment services on request and periodically checks in to ensure that deployment is on track and to help remove blockers.

The main phases of a typical FastTrack for Azure engagement are:

- **Discovery.** Identify key stakeholders, understand the goal or vision for problems to be solved, and then assess architectural needs.
- **Solution enablement.** Learn design principles for building applications, review architecture of applications and solutions, and receive guidance and tools to drive proof of concept (PoC) work through to production.
- **Continuous partnership.** Azure engineers and program managers check in every so often to ensure that deployment is on track and to help remove blockers.

## Microsoft Services offerings aligned to Cloud Adoption Framework approaches

# Microsoft Services Cloud Adoption Program Approach



**Assess:** Microsoft Services uses a [unified data- and tool-driven approach](#) consisting of architectural workshops, Azure real-time information, security and identity threat models and various tools to provide insights into challenges, risks, recommendations and issues to an existing Azure environment with a key outcome such as [high-level modernization roadmap](#).

**Adopt:** Using the [Azure cloud foundation](#) from Microsoft Services, establish your core Azure designs, patterns and governance architecture by mapping your requirements to the most appropriate reference architecture and plan, design and deploy the infrastructure, management, security, and identity required for workloads.

**Migrate/optimize:** The [cloud modernization solution](#) from Microsoft Services offers a comprehensive approach to move applications and infrastructure to Azure, as well as to optimize and modernize after cloud deployment, backed by streamlined migration.

**Innovate:** The [cloud center of excellence \(CCoE\) solution](#) from Microsoft Services offers a DevOps coaching engagement and uses DevOps principles combined with prescriptive cloud-native service management and security controls to help drive business innovation, increase agility, and reduce time to value within a secure, predictable, and flexible services delivery and operations management capability.

## Azure support

If you have questions or need help, [create a support request](#). If your support request requires deep technical guidance, visit [Azure support plans](#) to align the best plan for your needs.

## Azure solutions partner

Microsoft certified solution providers specialize in providing modern customer solutions based on Microsoft technologies across the world. Optimize your business in the cloud with help from an experienced partner.

Get help from partners with ready-made or custom Azure solutions and partners who can help deploy and manage those solutions:

- [Find a cloud solutions partner](#). A certified CSP can help take full advantage of the cloud by assessing business goals for cloud adoption, identifying the right cloud solution that meets business needs and helps the business become more agile and efficient.
- [Find an Azure Expert Managed Service Provider \(MSPs\)](#). MSPs help businesses transition to Azure by guiding all aspects of the cloud journey. From consulting to migrations and operations management, cloud MSPs show

customers all the benefits that come with cloud adoption. They also act as a one-stop shop for common support, provisioning, and the billing experience, all with a flexible pay-as-you-go business model.

## Next steps

After a partner and support strategy is selected, the [release and iteration backlogs](#) can be updated to reflect planned efforts and assignments.

[Manage change using release and iteration backlogs](#)

# Manage change in an incremental migration effort

11/9/2020 • 2 minutes to read • [Edit Online](#)

This article assumes that migration processes are incremental in nature, running parallel to the [govern process](#). However, the same guidance could be used to populate initial tasks in a work breakdown structure for traditional waterfall change management approaches.

## Release backlog

A *release backlog* consists of a series of assets (VMs, databases, files, and applications, among others) that must be migrated before a workload can be released for production usage in the cloud. During each iteration, the cloud adoption team documents and estimates the efforts required to move each asset to the cloud. See the "iteration backlog" section that follows.

## Iteration backlog

An *iteration backlog* is a list of the detailed work required to migrate a specific number of assets from the existing digital estate to the cloud. The entries on this list are often stored in an agile management tool, like Azure DevOps, as work items.

Prior to starting the first iteration, the cloud adoption team specifies an iteration duration, usually two to four weeks. This time box is important to create a start and finish time period for each set of committed activities. Maintaining consistent execution windows makes it easy to gauge velocity (pace of migration) and alignment to changing business needs.

Prior to each iteration, the team reviews the release backlog, estimating the effort and priorities of assets to be migrated. It then commits to deliver a specific number of agreed-on migrations. After this is agreed to by the cloud adoption team, the list of activities becomes the *current iteration backlog*.

During each iteration, team members work as a self-organizing team to fulfill commitments in the current iteration backlog.

## Next steps

After an iteration backlog is defined and accepted by the cloud adoption team, [change management approvals](#) can be finalized.

[Approve architecture changes prior to migration](#)

# Approve architecture changes before migration

11/9/2020 • 4 minutes to read • [Edit Online](#)

During the assess process of migration, each workload is evaluated, architected, and estimated to develop a future state plan for the workload. Some workloads can be migrated to the cloud with no change to the architecture. Maintaining on-premises configuration and architecture can reduce risk and streamline the migration process. Unfortunately, not every application can run in the cloud without changes to the architecture. When architecture changes are required, this article can help classify the change and can provide some guidance on the proper approval activities.

## Business impact and approval

During migration, some things are likely to change in ways that impact the business. Although change sometimes can't be avoided, surprises as a result of undisclosed or undocumented changes should be. To maintain stakeholder support throughout the migration effort, it's important to avoid surprises. Surprising application owners or business stakeholders can slow or halt a cloud adoption effort.

Prior to migration, it is important to prepare the workload's business owner for any changes that could affect business processes, such as changes to:

- Service-level agreements.
- Access patterns or security requirements that impact the end user.
- Data retention practices.
- Core application performance.

Even when a workload can be migrated with minimal to no change, there could still be a business impact. Replication processes can slow the performance of production systems. Changes to the environment in preparation for migration have the potential to cause routing or network performance limitations. There are many additional impacts that could result from replication, staging, or promotion activities.

Regular approval activities can help minimize or avoid surprises as a result of change or performance-driven business impacts. The cloud adoption team should execute a change approval process at the end of the assessment process, before beginning the migration process.

## Existing culture

Your IT teams likely have existing mechanisms for managing change involving your on-premises assets. Typically these mechanisms are governed by traditional Information Technology Infrastructure Library-based (ITIL-based) change management processes. In many enterprise migrations, these processes involve a change advisory board (CAB) that's responsible for reviewing, documenting, and approving all IT-related requests for changes (RFC).

The CAB generally includes experts from multiple IT and business teams, offering a variety of perspectives and detailed review for all IT-related changes. A CAB approval process is a proven way to reduce risk and minimize the business impact of changes involving stable workloads managed by IT operations.

## Technical approval

Organizational readiness for the approval of technical change is among the most common reasons for cloud migration failure. More projects are stalled by a series of technical approvals than any deficit in a cloud platform. Preparing the organization for technical change approval is an important requirement for migration success. The following are a few best practices to ensure that the organization is ready for technical approval.

## **ITIL change advisory board challenges**

Every change management approach has its own set of controls and approval processes. Migration is a series of continuous changes that start with a high degree of ambiguity and develop additional clarity through the course of execution. As such, migration is best governed by agile-based change management approaches, with the cloud strategy team serving as a product owner.

However, the scale and frequency of change during a cloud migration doesn't fit well with the nature of ITIL processes. The requirements of a CAB approval can risk the success of a migration, slowing or stopping the effort. Further, in the early stages of migration, ambiguity is high and subject matter expertise tends to be low. For the first several workload migrations or releases, the cloud adoption team is often in a learning mode. As such, it could be difficult for the team to provide the types of data needed to pass a CAB approval.

The following best practices can help the CAB maintain a degree of comfort during migration without become a painful blocker.

### **Standardize change**

It is tempting for a cloud adoption team to consider detailed architectural decisions for each workload being migrated to the cloud. It is equally tempting to use cloud migration as a catalyst to refactor past architectural decisions. For organizations that are migrating a few hundred VMs or a few dozen workloads, either approach can be properly managed. When migrating a datacenter consisting of 1,000 or more assets, each of these approaches is considered a high-risk antipattern that significantly reduces the likelihood of success. Modernizing, refactoring, and rearchitecting every application requires a diverse skill set and a wide variety of changes, and these tasks create dependencies on human efforts at scale. Each of these dependencies injects risk into the migration effort.

The article on [digital estate rationalization](#) discusses the agility and time-saving impact of basic assumptions when rationalizing a digital estate. There is an additional benefit of standardized change. By choosing a default rationalization approach to govern the migration effort, the cloud advisory board or product owner can review and approve the application of one change to a long list of workloads. This reduces technical approval of each workload to those that require a significant architecture change to be cloud compatible.

### **Clarify expectations and roles of approvers**

Before the first workload is assessed, the cloud strategy team should document and communicate the expectations of anyone involved in the approval of change. This simple activity can avoid costly delays when the cloud adoption team is fully engaged.

### **Seek approval early**

When possible, technical change should be detected and documented during the assessment process. Regardless of approval processes, the cloud adoption team should engage approvers early. The sooner that change approval can begin, the less likely an approval process is to block migration activities.

## **Next steps**

With the help of these best practices, it should be easier to integrate proper, low-risk approval into migration efforts. After workload changes are approved, the cloud adoption team is ready to migrate workloads.

### [\*\*Migrate workloads\*\*](#)

# Deploy workloads

11/9/2020 • 2 minutes to read • [Edit Online](#)

After workloads have been assessed, they can be deployed to the cloud or staged for release. This series of articles explains the various activities that may be involved in this phase of migration effort.

## Objective

The objective of a migration is to migrate a single workload to the cloud.

## Definition of done

The migration phase is complete when a workload is staged and ready for testing in the cloud, including all dependent assets required for the workload to function. During the optimize process, the workload is prepared for production usage.

This *definition of done* can vary, depending on your testing and release processes. The next article in this series covers [deciding on a promotion model](#) and can help you understand when it would be best to promote a migrated workload to production.

## Accountability during migration

The cloud adoption team is accountable for the entire migration process. However, members of the cloud strategy team have a few responsibilities, as discussed in the following section.

## Responsibilities during migration

In addition to the high-level accountability, there are actions that an individual or group needs to be directly responsible for. The following are a few activities that require assignments to responsible parties:

- **Remediation.** Resolve any compatibility issues that prevent the workload from being migrated to the cloud.
  - As discussed in the prerequisite article regarding [technical complexity and change management](#), a decision should be made in advance to determine how this activity is to be executed. In particular, will remediation be completed by the cloud adoption team during the same sprint as the actual migration effort? Alternatively, will a wave or factory model be used to complete remediation in a separate iteration? If the answer to this basic process question can't be answered by every member of the team, it may be wise to revisit the section on [prerequisites](#).
- **Replication.** Create a copy of each asset in the cloud to synchronize VMs, data, and applications with resources in the cloud.
  - Depending on the promotion model, different tools may be required to complete this activity.
- **Staging.** After all assets for a workload have been replicated and verified, the workload can be staged for business testing and execution of a business change plan.

## Next steps

With a general understanding of the migration process, you're ready to [decide on a promotion model](#).

[Decide on a promotion model](#)

# Promotion models: Single-step, staged, or flight

11/9/2020 • 5 minutes to read • [Edit Online](#)

Workload migration is often discussed as a single activity. In practice, it's a collection of smaller activities that facilitate the movement of a digital asset to the cloud. One of the last activities in a migration is the promotion of an asset to production. Promotion is the point at which the production system changes for end users. It can often be as simple as changing the network routing, redirecting end users to the new production asset. Promotion is also the point at which IT operations or cloud operations change the focus of operational management processes from the previous production system to the new production systems.

There are several promotion models. This article outlines three of the most common ones used in cloud migrations. The choice of a promotion model changes the activities seen within the migrate and optimize processes. As such, promotion model should be decided early in a release.

## Impact of promotion model on migrate and optimize activities

In each of the following promotion models, the chosen migration tool replicates and stages the assets that make up a workload. After staging, each model treats the asset a bit differently.

- **Single-step promotion.** In a *single-step* promotion model, the staging process doubles as the promotion process. After all assets are staged, end-user traffic is rerouted and staging becomes production. In such a case, promotion is part of the migration process. This is the fastest migration model. However, this approach makes it more difficult to integrate robust testing or optimization activities. Further, this type of model assumes that the migration team has access to the staging and production environment, which compromises separation of duties in some environments.

### NOTE

The table of contents for this site lists the promotion activity as part of the optimize process. In a single-step model, promotion occurs during the Migrate phase. When using this model, roles and responsibilities should be updated to reflect this.

- **Staged.** In a *staged* promotion model, the workload is considered migrated after it is staged, but it is not yet promoted. Prior to promotion, the migrated workload undergoes a series of performance tests, business tests, and optimization changes. It is then promoted at a future date in conjunction with a business test plan. This approach improves the balance between cost and performance, while making it easier to obtain business validation.
- **Flight.** The *flight* promotion model combines single-step and staged models. In a flight model, the assets in the workload are treated like production after landing in staging. After a condensed period of automated testing, production traffic is routed to the workload. However, it is a subset of the traffic. That traffic serves as the first flight of production and testing. Assuming the workload performs from a feature and performance perspective, additional traffic is migrated. After all production traffic has been moved onto the new assets, the workload is considered fully promoted.

The chosen promotion model affects the sequence of activities to be performed. It also affects the roles and responsibilities of the cloud adoption team. It may even impact the composition of a sprint or multiple sprints.

## Single-step promotion

This model uses migration automation tools to replicate, stage, and promote assets. The assets are replicated into

a contained staging environment controlled by the migration tool. After all assets have been replicated, the tool can execute an automated process to promote the assets into the chosen subscription in a single step. While in staging, the tool continues to replicate the asset, minimizing loss of data between the two environments. After an asset is promoted, the linkage between the source system and the replicated system is severed. In this approach, if additional changes occur in the initial source systems, the changes are lost.

**Pros.** Positive benefits of this approach include:

- This model introduces less change to the target systems.
- Continuous replication minimizes data loss.
- If a staging process fails, it can quickly be deleted and repeated.
- Replication and repeated staging tests enable an incremental scripting and testing process.

**Cons.** Negative aspects of this approach include:

- Assets staged within the tools-isolated sandbox don't allow for complex testing models.
- During replication, the migration tool consumes bandwidth in the local datacenter. Staging a large volume of assets over an extended duration has an exponential impact on available bandwidth, hurting the migration process and potentially affecting performance of production workloads in the on-premises environment.

## Staged promotion

In this model, the staging sandbox managed by the migration tool is used for limited testing purposes. The replicated assets are then deployed into the cloud environment, which serves as an extended staging environment. The migrated assets run in the cloud, while additional assets are replicated, staged, and migrated. When full workloads become available, richer testing is initiated. When all assets associated with a subscription have been migrated, the subscription and all hosted workloads are promoted to production. In this scenario, there is no change to the workloads during the promotion process. Instead, the changes tend to be at the network and identity layers, routing users to the new environment and revoking access of the cloud adoption team.

**Pros.** Positive benefits of this approach include:

- This model provides more accurate business testing opportunities.
- The workload can be studied more closely to better optimize performance and cost of the assets.
- A larger numbers of assets can be replicated within similar time and bandwidth constraints.

**Cons.** Negative aspects of this approach include:

- The chosen migration tool can't facilitate ongoing replication after migration.
- A secondary means of data replication is required to synchronize data platforms during the staged time frame.

## Flight promotion

This model is similar to the staged promotion model. However, there is one fundamental difference. When the subscription is ready for promotion, end-user routing happens in stages or flights. At each flight, additional users are rerouted to the production systems.

**Pros.** Positive benefits of this approach include:

- This model mitigates the risks associated with a big migration or promotion activity. Errors in the migrated solution can be identified with less impact to business processes.
- It allows for monitoring of workload performance demands in the cloud environment for an extended duration, increasing accuracy of asset-sizing decisions.
- Larger numbers of assets can be replicated within similar time and bandwidth constraints.

**Cons.** Negative aspects of this approach include:

- The chosen migration tool can't facilitate ongoing replication after migration.
- A secondary means of data replication is required to synchronize data platforms during the staged time frame.

## Next steps

After a promotion model is defined and accepted by the cloud adoption team, [remediation of assets](#) can begin.

[Remediating assets prior to migration](#)

# Remediate assets prior to migration

11/9/2020 • 4 minutes to read • [Edit Online](#)

During the assessment process of migration, the team seeks to identify any configurations that would make an asset incompatible with the chosen cloud provider. *Remediate* is a checkpoint in the migration process to ensure that those incompatibilities have been resolved. This article discusses a few common remediation tasks for reference. It also establishes a skeleton process for deciding whether remediation is a wise investment.

## Common remediation tasks

In any corporate environment, technical debt exists. Some of this is healthy and expected. Architecture decisions that were well suited for an on-premises environment may not be entirely suitable in a cloud platform. In either case, common remediation tasks may be required to prepare assets for migration. The following are a few examples:

- **Minor host upgrades.** Occasionally, an outdated host needs to be upgraded prior to replication.
- **Minor guest OS upgrades.** It is more likely that an OS will need patching or upgrading prior to replication.
- **SLA modifications.** Backup and recovery change significantly in a cloud platform. It is likely that assets will need minor modifications to their backup processes to ensure continued function in the cloud.
- **PaaS migration.** In some cases, a PaaS deployment of a data structure or application may be required to accelerate deployment. Minor modifications may be required to prepare the solution for PaaS deployment.
- **PaaS code changes.** It is not uncommon for custom applications to require minor code modifications to be PaaS ready. Examples could include methods that write to local disk or use of in-memory session state, among others.
- **Application configuration changes.** Migrated applications may require changes to variables, such as network paths to dependent assets, service account changes, or updates to dependent IP addresses.
- **Minor changes to network paths.** Routing patterns may need to be modified to properly route user traffic to the new assets.

### NOTE

This isn't production routing to the new assets, but rather configuration to allow for proper routing to the assets in general.

## Large-scale remediation tasks

When a datacenter is properly maintained, patched, and updated, there is likely to be little need for remediation. Remediation-rich environments tend to be common among large enterprises, organizations that have been through large IT downsizing, some legacy managed service environments, and acquisition-rich environments. In each of these types of environments, remediation may consume a large portion of the migration effort. When the following remediation tasks frequently appear and are negatively affecting migration speed or consistency, it may be wise to break out remediation into a parallel effort and team (similar to how cloud adoption and cloud governance run in parallel).

- **Frequent host upgrades.** When large numbers of hosts must be upgraded to complete the migration of a workload, the migration team is likely to suffer from delays. It may be wise to break out affected applications and address the remediation steps prior to including affected applications in any planned releases.
- **Frequent guest OS upgrade.** Large enterprises commonly have servers running on outdated versions of Linux or Windows. Aside from the apparent security risks of operating an outdated OS, there are also

incompatibility issues that prevent affected workloads from being migrated. When a large number of VMs require OS remediation, it may be wise to break out these efforts into a parallel iteration.

- **Major code changes.** Older custom applications may require significantly more modifications to prepare them for PaaS deployment. When this is the case, it may be wise to remove them from the migration backlog entirely, managing them in a wholly separate program.

## Decision framework

Because remediation for smaller workloads can be straightforward, you should choose a smaller workload for your initial migration. However, as your migration efforts mature and you begin to tackle larger workloads, remediation can be a time consuming and costly process. For example, remediation efforts for a Windows Server 2003 migration involving a 5,000+ VM pool of assets can delay a migration by months. When such large-scale remediation is required, the following questions can help guide decisions:

- Have all workloads affected by the remediation been identified and notated in the migration backlog?
- For workloads that are not affected, will a migration produce a similar return on investment (ROI)?
- Can the affected assets be remediated in alignment with the original migration timeline? What impact would timeline changes have on ROI?
- Is it economically feasible to remediate the assets in parallel with migration efforts?
- Is there sufficient bandwidth on staff to remediate and migrate? Should a partner be engaged to execute one or both tasks?

If these questions don't yield favorable answers, a few alternative approaches that move beyond a basic IaaS rehosting strategy may be worth considering:

- **Containerization.** Some assets can be hosted in a containerized environment without remediation. This could produce less-than-favorable performance and doesn't resolve security or compliance issues.
- **Automation.** Depending on the workload and remediation requirements, it may be more profitable to script the deployment to new assets using a DevOps approach.
- **Rebuild.** When remediation costs are very high and business value is equally high, a workload may be a good fit as a candidate for rebuilding or rearchitecting.

## Next steps

After remediation is complete, [replication activities](#) are ready.

[Replicate assets](#)

# What role does replication play in the migration process?

11/9/2020 • 4 minutes to read • [Edit Online](#)

On-premises datacenters are filled with physical assets like servers, appliances, and network devices. However, each server is only a physical shell. The real value comes from the binary running on the server. The applications and data are the purpose for the datacenter. Those are the primary binaries to migrate. Powering these applications and data stores are other digital assets and binary sources, like operating systems, network routes, files, and security protocols.

Replication is the workhorse of migration efforts. It is the process of copying a point-in-time version of various binaries. The binary snapshots are then copied to a new platform and deployed onto new hardware, in a process referred to as *seeding*. When executed properly, the seeded copy of the binary should behave identically to the original binary on the old hardware. However, that snapshot of the binary is immediately out of date and misaligned with the original source. To keep the new binary and the old binary aligned, a process referred to as *synchronization* continuously updates the copy stored in the new platform. Synchronization continues until the asset is promoted in alignment with the chosen promotion model. At that point, the synchronization is severed.

## Required prerequisites to replication

Prior to replication, the new platform and hardware must be prepared to receive the binary copies. The article on [prerequisites](#) outlines minimum environment requirements to help create a safe, robust, high-performance platform to receive the binary replicas.

The *source binaries* must also be prepared for replication and synchronization. The articles on assessment, architecture, and remediation each address the actions necessary to ensure that the source binary is ready for replication and synchronization.

A *toolchain* that aligns with the new platform and source binaries must be implemented to execute and manage the replication and synchronization processes. The article on [replication options](#) outlines various tools that could contribute to a migration to Azure.

## Replication risks - physics of replication

When planning for the replication of any binary source to a new destination, there are a few fundamental laws to seriously consider during planning and execution.

- **Speed of light.** When moving high volumes of data, fiber is still the fastest option. Unfortunately, those cables can only move data at two-thirds the speed of light. This means that there is no method for instantaneous or unlimited replication of data.
- **Speed of WAN pipeline.** More consequential than the speed of data movement is the uplink bandwidth, which defines the volume of data per second that can be carried over a company's existing WAN to the target datacenter.
- **Speed of WAN expansion.** If budgets allow, additional bandwidth can be added to a company's WAN solution. However, it can take weeks or months to procure, provision, and integrate additional fiber connections.
- **Speed of disks.** If data could move faster and there was no limit to the bandwidth between the source binary and the target destination, physics would still be a limiter. Data can be replicated only as quickly as it can be read from source disks. Reading every one or zero from every spinning disk in a datacenter takes time.

- **Speed of human calculations.** Disks and light move faster than human decision processes. When a group of humans is required to collaborate and make decisions together, the results will come even more slowly. Replication can never overcome delays related to human intelligence.

Each of these laws of physics drive the following risks that commonly affect migration plans:

- **Replication time.** Replication requires time and bandwidth. Plans should include realistic timelines that reflect the amount of time it takes to replicate binaries. *Total available migration bandwidth* is the amount of up-bound bandwidth, measured in megabits per second (Mbps) or gigabits per second (Gbps), that is not consumed by other higher priority business needs. *Total migration storage* is the total disk space, measured in gigabytes or terabytes, required to store a snapshot of all assets to be migrated. An initial estimate of time can be calculated by dividing the *total migration storage* by *total available migration bandwidth*. Note the conversion from bits to bytes. See the following entry, "cumulative effect of disk drift," for a more accurate calculation of time.
- **Cumulative effect of disk drift.** From the point of replication to the promotion of an asset to production, the source and destination binaries must remain synchronized. *Drift* in binaries consumes additional bandwidth, as all changes to the binary must be replicated on a recurring basis. During synchronization, all binary drift must be included in the calculation for total migration storage. The longer it takes to promote an asset to production, the more cumulative drift will occur. The more assets being synchronized, the more bandwidth consumed. With each asset being held in a synchronization state, a bit more of the total available migration bandwidth is lost.
- **Time to business change.** As mentioned previously, synchronization time has a cumulative negative effect on migration speed. Prioritization of the migration backlog and advanced preparation for the [business change plan](#) are crucial to the speed of migration. The most significant test of business and technical alignment during a migration effort is the pace of promotion. The faster an asset can be promoted to production, the less impact disk drift will have on bandwidth and the more bandwidth/time that can be allocated to replication of the next workload.

## Next steps

After replication is complete, [staging activities](#) can begin.

[Staging activities during a migration](#)

# Replication options

11/9/2020 • 2 minutes to read • [Edit Online](#)

Before any migration, you should ensure that primary systems are safe and will continue to run without issues. Any downtime disrupts users or customers, and it costs time and money. Migration is not as simple as turning off the virtual machines on-premises and copying them across to Azure. Migration tools must take into account asynchronous or synchronous replication to ensure that live systems can be copied to Azure with no downtime. Most of all, systems must be kept in lockstep with on-premises counterparts. You might want to test migrated resources in isolated partitions in Azure, to ensure that workloads work as expected.

The content within the Cloud Adoption Framework assumes that Azure Migrate (or Azure Site Recovery) is the most appropriate tool for replicating assets to the cloud. However, there are other options available. This article discusses those options to help enable decision-making.

## Azure Site Recovery (also known as Azure Migrate)

[Azure Site Recovery](#) orchestrates and manages disaster recovery for Azure VMs, on-premises VMs, and physical servers. You can also use Site Recovery to manage migration of machines on-premises and other cloud providers to Azure. Replicate on-premises machines to Azure or Azure VMs to a secondary region. Then, you fail the VM over from the primary site to the secondary and complete the migration process. With Azure Site Recovery, you can achieve various migration scenarios:

- **Migrate from on-premises to Azure.** Migrate on-premises VMware VMs, Hyper-V VMs, and physical servers to Azure. To do this, complete almost the same steps as you would for full disaster recovery. Simply don't fail machines back from Azure to the on-premises site.
- **Migrate between Azure regions.** Migrate Azure VMs from one Azure region to another. After the migration is complete, configure disaster recovery for the Azure VMs now in the secondary region to which you migrated.
- **Migrate from other cloud to Azure.** You can migrate your compute instances provisioned on other cloud providers to Azure VMs. Site Recovery treats those instances as physical servers for migration purposes.

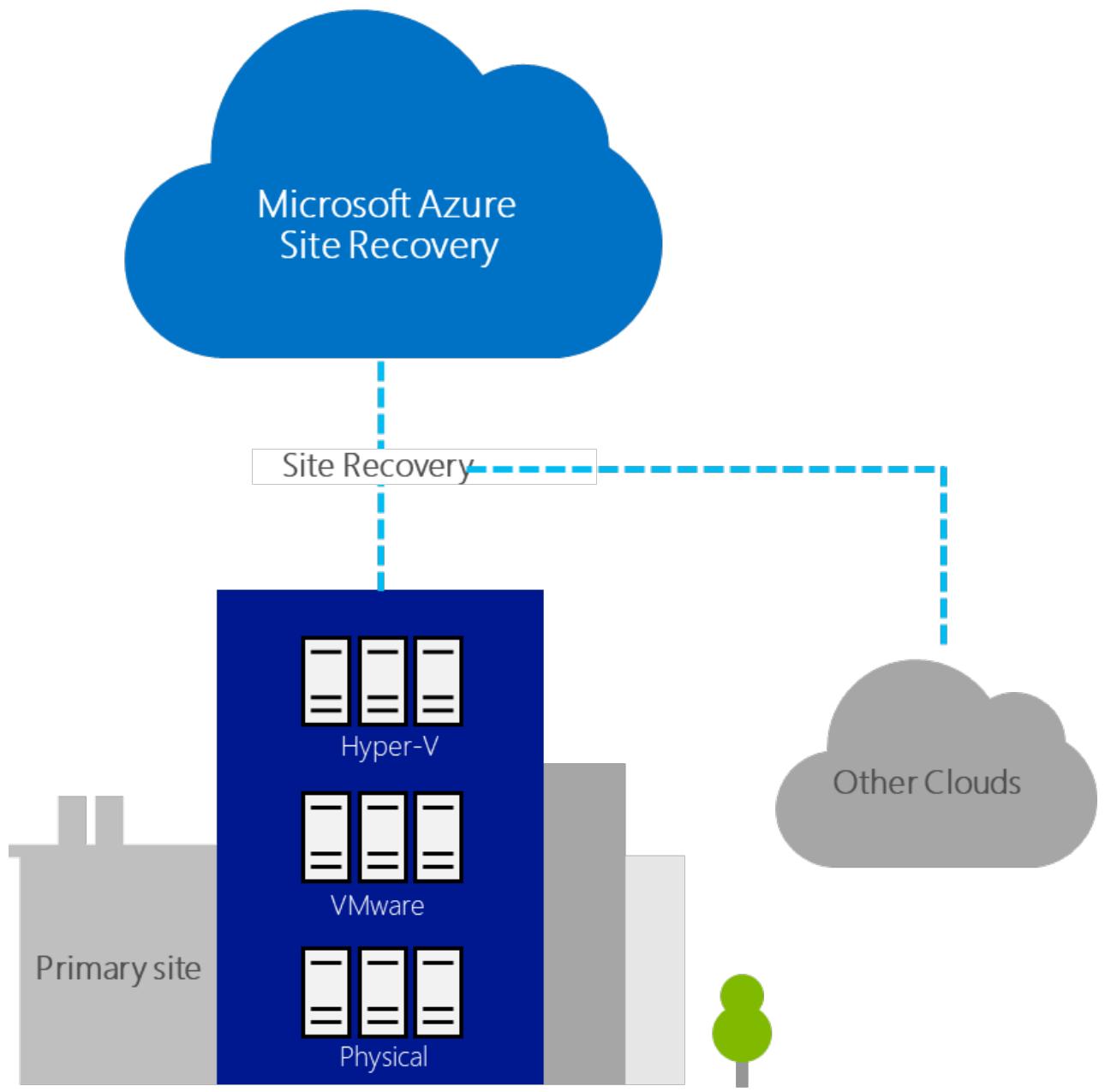


Figure 1: Azure Site Recovery moving assets to Azure or other clouds.

After you have assessed on-premises and cloud infrastructure for migration, Azure Site Recovery contributes to your migration strategy by replicating on-premises machines. With the following easy steps, you can set up migration of on-premises VMs, physical servers, and cloud VM instances to Azure:

- Verify prerequisites.
- Prepare Azure resources.
- Prepare on-premises VM or cloud instances for migration.
- Deploy a configuration server.
- Enable replication for VMs.
- Test failover to make sure everything's working.
- Run a one-time failover to Azure.

## Azure Database Migration Service

This service helps reduce the complexity of your cloud migration by using a single comprehensive service instead of multiple tools. [Azure Database Migration Service](#) is designed as a seamless, end-to-end solution for moving on-premises SQL Server databases to the cloud. It is a fully managed service designed to enable seamless migrations from multiple database sources to Azure data platforms with minimal downtime. It integrates some of the functionality of existing tools and services, providing customers with a comprehensive, highly available solution.

The service uses Data Migration Assistant to generate assessment reports that provide recommendations to guide you through the changes required prior to performing a migration. It's up to you to perform any required remediation. When you're ready to begin the migration process, Azure Database Migration Service performs all of the associated steps. You can fire and forget your migration projects with peace of mind, knowing that the process takes advantage of best practices as determined by Microsoft.

## Next steps

After replication is complete, [staging activities](#) can begin.

[Staging activities during a migration](#)

# Understand staging activities during a migration

11/9/2020 • 2 minutes to read • [Edit Online](#)

As described in the article on promotion models, *staging* is the point at which assets have been migrated to the cloud. However, they're not ready to be promoted to production yet. This is often the last step in the migrate process of a migration. After staging, the workload is managed by an IT operations or cloud operations team to prepare it for production usage.

## Deliverables

Staged assets may not be ready for use in production. There are several production readiness checks that should be finalized before this stage is considered complete. The following is a list of deliverables often associated with completion of asset staging.

- **Automated testing.** Any automated tests available to validate workload performance should be run before concluding the staging process. After the asset leaves staging, synchronization with the original source system is terminated. As such, it is harder to redeploy the replicated assets, after the assets are staged for optimization.
- **Migration documentation.** Most migration tools can produce an automated report of the assets being migrated. Before concluding the staging activity, all migrated assets should be documented for clarity.
- **Configuration documentation.** Any changes made to an asset (during remediation, replication, or staging) should be documented for operational readiness.
- **Backlog documentation.** The migration backlog should be updated to reflect the workload and assets staged.

## Next steps

After staged assets are tested and documented, you can proceed to optimization activities.

[Optimize migrated workloads](#)

# Release workloads

11/9/2020 • 2 minutes to read • [Edit Online](#)

After a collection of workloads and their supporting assets have been deployed to the cloud, it must be prepared before it can be released. In this phase of the migration effort, the collection of workloads are load tested and validated with the business. They're then optimized and documented. Once the business and IT teams have reviewed and signed off on workload deployments, those workloads can be released or handed off to governance, security, and operations teams for ongoing operations.

The objective of "release workloads" is to prepare migrated workloads for promotion to production usage.

## Definition of done

The optimization process is complete when a workload has been properly configured, sized, and deployed to production.

## Accountability during optimization

The cloud adoption team is accountable for the entire optimization process. However, members of the cloud strategy team, the cloud operations team, and the cloud governance team should also be responsible for activities within this process.

## Responsibilities during optimization

In addition to the high-level accountability, there are actions that an individual or group needs to be directly responsible for. The following are a few activities that require assignments to responsible parties:

- **Business testing.** Resolve any compatibility issues that prevent the workload from completing its migration to the cloud.
  - Power users from within the business should participate heavily in testing of the migrated workload. Depending on the degree of optimization attempted, multiple testing cycles may be required.
- **Business change plan.** Development of a plan for user adoption, changes to business processes, and modification to business KPIs or learning metrics as a result of the migration effort.
- **Benchmark and optimize.** Study of the business testing and automated testing to benchmark performance. Based on usage, the cloud adoption team refines sizing of the deployed assets to balance cost and performance against expected production requirements.
- **Ready for production.** Prepare the workload and environment for the support of the workload's ongoing production usage.
- **Promote.** Redirect production traffic to the migrated and optimized workload. This activity represents the completion of a release cycle.

In addition to core activities, there are a few parallel activities that require specific assignments and execution plans:

- **Decommission.** Generally, cost savings can be realized from a migration, when the previous production assets are decommissioned and properly disposed of.
- **Retrospective.** Every release creates an opportunity for deeper learning and adoption of a growth mindset. When each release cycle is completed, the cloud adoption team should evaluate the processes used during migration to identify improvements.

## Next steps

With a general understanding of the optimization process, you're ready to begin the process by [establishing a business change plan for the candidate workload](#).

[Business change plan](#)

# Business change plan

11/9/2020 • 3 minutes to read • [Edit Online](#)

Traditionally, IT has overseen the release of new workloads. During a major transformation, like a datacenter migration or a cloud migration, a similar pattern of IT lead adoption could be applied. However, the traditional approach might miss opportunities to realize additional business value. For this reason, before a migrated workload is promoted to production, implementing a broader approach to user adoption is suggested. This article outlines the ways in which a business change plan adds to a standard user adoption plan.

## Traditional user adoption approach

User adoption plans focus on how users will adopt a new technology or change to a given technology. This approach is time tested for introducing users to new tools. In a typical user adoption plan, IT focuses on the installation, configuration, maintenance, and training associated with the technical changes being introduced to the business environment.

Although approaches may vary, general themes are present in most user adoption plans. These themes are typically based on a risk control and facilitation approach that aligns to incremental improvement. The Eason Matrix, illustrated in the figure below, represents the drivers behind those themes across a spectrum of adoption types.

		Revolution → Evolution		
Adoption type		Big Bang	Parallel Running	Phased adoption
Criteria	Needed "critical mass"	Big	Small	
	Need for risk control	Low	High	
Need for facilitation of the change	Low	High		
	Pace of change over Local design needs	High	Low	
User adaptation	Difficult	→ Easy		

Diagram: Eason Matrix

of user adoption types.

These themes are often based on the assumption that introduction of new solutions to users should focus largely on risk control and facilitation of change. Additionally, IT has focused mostly on risk from the technology change and facilitation of that change.

## Create business change plans

A business change plan looks beyond the technical change and assumes that every release in a migration effort drives some level of business process change. It looks upstream and downstream from the technical changes. The following questions help participants think about user adoption from a business change perspective, to maximize business impact:

**Upstream questions.** Upstream questions look at impacts or changes that come before user adoption happens:

- Has an expected [business outcome](#) been quantified?
- Does the business impact map to defined [learning metrics](#)?

- Which business processes and teams take advantage of this technical solution?
- Who in the business can best align power users for testing and feedback?
- Have the affected business leaders been involved in the prioritization and migration planning?
- Are there any critical events or dates for the business that could be affected by this change?
- Does the business change plan maximize impact but minimize business disruption?
- Is downtime expected? Has a downtime window been communicated to end users?

**Downstream questions.** After the adoption is complete, the business change can begin. Unfortunately, this is where many user adoption plans end. Downstream questions help the cloud strategy team maintain a focus on transformation after technical change is completed:

- Are business users responding well to the changes?
- Has performance anticipation been maintained, now that the technical change has been adopted?
- Are business processes or customer experiences changing in the anticipated ways?
- Are additional changes required to realize learning metrics?
- Did the changes align to the targeted business outcomes? If not, why not?
- Are additional changes required to contribute to business outcomes?
- Have any negative effects been observed as a result of this change?

The business change plan varies from company to company. The goal of these questions is to help better integrate the business into the change associated with each release. By looking at each release not as a technology change to be adopted but instead as a business change plan, business outcomes can become more obtainable.

## Next steps

After business change is documented and planned, [business testing](#) can begin.

[Guidance for business testing \(UAT\) during migration](#)

## References

- Eason, K. (1988) *Information Technology and Organizational Change*, New York: Taylor and Francis.

# Guidance for business testing (UAT) during migration

3/31/2020 • 3 minutes to read • [Edit Online](#)

Traditionally seen as an IT function, user acceptance testing during a business transformation can be orchestrated solely by IT. However, this function is often most effectively executed as a business function. IT then supports this business activity by facilitating the testing, developing testing plans, and automating tests when possible. Although IT can often serve as a surrogate for testing, there is no replacement for firsthand observation of real users attempting to take advantage of a new solution in the context of a real or replicated business process.

## NOTE

When available, automated testing is a much more effective and efficient means of testing any system. However, cloud migrations often focus most heavily on legacy systems or at least stable production systems. Often, those systems aren't managed by thorough and well-maintained automated tests. This article assumes that no such tests are available at the time of migration.

Second to automated testing is testing of the process and technology changes by power users. Power users are the people that commonly execute a real-world process that requires interactions with a technology tool or set of tools. They could be represented by an external customer using an e-commerce site to acquire goods or services. Power users could also be represented by a group of employees executing a business process, such as a call center servicing customers and recording their experiences.

The goal of business testing is to solicit validation from power users to certify that the new solution performs in line with expectations and does not impede business processes. If that goal isn't met, the business testing serves as a feedback loop that can help define why and how the workload isn't meeting expectations.

## Business activities during business testing

During business testing, the first iteration is manually driven directly with customers. This is the purest but most time-consuming form of feedback loop.

- **Identify power users.** The business generally has a better understanding of the power users who are most affected by a technical change.
- **Align and prepare power users.** Ensure that power users understand the business objectives, desired outcomes, and expected changes to business processes. Prepare them and their management structure for the testing process.
- **Engage in feedback loop interpretation.** Help the IT staff understand the impact of various points of feedback from power users.
- **Clarify process change.** When transformation could trigger a change to business processes, communicate the change and any downstream impacts.
- **Prioritize feedback.** Help the IT team prioritize feedback based on the business impact.

At times, IT may employ analysts or product owners who can serve as proxies for the itemized business testing activities. However, business participation is highly encouraged and is likely to produce favorable business outcomes.

## IT activities during business testing

IT serves as one of the recipients of the business testing output. The feedback loops exposed during business testing eventually become work items that define technical change or process change. As a recipient, IT is expected

to aid in facilitation, collection of feedback, and management of resultant technical actions. The typical activities IT performs during business testing include:

- Provide structure and logistics for business testing.
- Aid in facilitation during testing.
- Provide a means and process for recording feedback.
- Help the business prioritize and validate feedback.
- Develop plans for acting on technical changes.
- Identify existing automated tests that could streamline the testing by power users.
- For changes that could require repeated deployment or testing, study testing processes, define benchmarks, and create automation to further streamline power user testing.

## Next steps

In conjunction with business testing, [optimization of migrated assets](#) can refine cost and workload performance.

[Benchmark and resize cloud assets](#)

# Benchmark and resize cloud assets

11/9/2020 • 3 minutes to read • [Edit Online](#)

Monitoring usage and spending is critically important for cloud infrastructures. Organizations pay for the resources they consume over time. When usage exceeds agreement thresholds, unexpected cost overages can quickly accumulate. Cost management reports monitor spending to analyze and track cloud usage, costs, and trends. Using overtime reports, detect anomalies that differ from normal trends. Inefficiencies in cloud deployment are visible in optimization reports. Note inefficiencies in cost-analysis reports.

In the traditional on-premises models of IT, requisition of IT systems is costly and time consuming. The processes often require lengthy capital expenditure review cycles and may even require an annual planning process. As such, it is common practice to buy more than is needed. It is equally common for IT administrators to then overprovision assets in preparation for anticipated future demands.

In the cloud, the accounting and provisioning models eliminate the time delays that lead to overbuying. When an asset needs additional resources, it can be scaled up or out almost instantly. This means that assets can safely be reduced in size to minimize resources and costs consumed. During benchmarking and optimization, the cloud adoption team seeks to find the balance between performance and costs, provisioning assets to be no larger and no smaller than necessary to meet production demands.

## Should assets be optimized during or after the migration?

Should an asset be optimized during or after the migration? The simple answer is **both**. However, that's not entirely accurate. To explain, take a look at two basic scenarios for optimizing resource sizing:

- **Planned resizing.** Often, an asset is clearly oversized and underutilized and should be resized during deployment. Determining if an asset has been successfully resized in this case requires user acceptance testing after migration. If a power user does not experience performance or functionality losses during testing, you can conclude the asset has been successfully sized.
- **Optimization.** In cases where the need for optimization is unclear, IT teams should use a data-driven approach to resource size management. Using benchmarks of the asset's performance, an IT team can make educated decisions regarding the most appropriate size, services, scale, and architecture of a solution. They can then resize and test performance theories post-migration.

During the migration, use educated guesses and experiment with sizing. However, true optimization of resources requires data based on actual performance in a cloud environment. For true optimization to occur, the IT team must first implement approaches to monitoring performance and resource utilization.

## Benchmark and optimize with Azure Cost Management and Billing

[Azure Cost Management and Billing](#) manages cloud spend with transparency and accuracy. This service monitors, benchmarks, allocates, and optimizes cloud costs.

Historical data can help manage costs by analyzing usage and costs over time to identify trends, which are then used to forecast future spending. Cost management also includes useful projected cost reports. Cost allocation manages costs by analyzing costs based on tagging policies. Use cost allocation for showback/chargeback to show resource utilization and associated costs to influence consumption behaviors or charge tenant customers. Access control helps manage costs by ensuring that users and teams access only the cost management data that they need. Alerting helps manage costs through automatic notification when unusual spending or overspending occurs. Alerts can also notify other stakeholders automatically for spending anomalies and overspending risks. Various reports support alerts based on budget and cost thresholds.

## Improve efficiency

Determine optimal VM usage, identify idle VMs, or remove idle VMs and unattached disks using Cost Management and Billing. Using information in sizing optimization and inefficiency reports, create a plan to downsize or remove idle VMs.

## Next steps

After a workload has been tested and optimized, it is time to [ready the workload for promotion](#).

[Getting a migrated workload ready for production promotion](#)

# Prepare a migrated application for production promotion

5/12/2020 • 2 minutes to read • [Edit Online](#)

After a workload is promoted, production user traffic is routed to the migrated assets. Readiness activities provide an opportunity to prepare the workload for that traffic. The following are a few business and technology considerations to help guide readiness activities.

## Validate the business change plan

Transformation happens when business users or customers take advantage of a technical solution to execute processes that drive the business. Readiness is a good opportunity to validate the [business change plan](#) and to ensure proper training for the business and technical teams involved. In particular, ensure that the following technology-related aspects of the change plan are properly communicated:

- End-user training is completed (or at least planned).
- Any outage windows have been communicated and approved.
- Production data has been synchronized and validated by end users.
- Validate promotion and adoption timing; ensure timelines and changes have been communicated to end users.

## Final technical readiness tests

*Ready* is the last step prior to production release. That means it is also the last chance to test the workload. The following are a few tests that are suggested during this phase:

- **Network isolation testing.** Test and monitor network traffic to ensure proper isolation and no unexpected network vulnerabilities. Also validate that any network routing to be severed during cutover is not experiencing unexpected traffic.
- **Dependency testing.** Ensure that all workload application dependencies have been migrated and are accessible from the migrated assets.
- **Business continuity and disaster recovery (BCDR) testing.** Validate that any backup and recovery SLAs are established. If possible, perform a full recovery of the assets from the BCDR solution.
- **End-user route testing.** Validate traffic patterns and routing for end-user traffic. Ensure that network performance aligns with expectations.
- **Final performance check.** Ensure that performance testing has been completed and approved by end users. Execute any automated performance testing.

## Final business validation

After the business change plan and technical readiness have been validated, the following final steps can complete the business validation:

- **Cost validation (plan versus actual).** Testing is likely to produce changes in sizing and architecture. Ensure that actual deployment pricing still aligns with the original plan.
- **Communicate and execute cutover plan.** Prior to cutover, communicate the cutover and execute accordingly.

## Next steps

After all readiness activities have been completed, its time to [promote the workload](#).

What is required to promote a migrated resource to production?

# What is required to promote a migrated resource to production?

11/9/2020 • 2 minutes to read • [Edit Online](#)

Promotion to production marks the completion of a workload's migration to the cloud. After the asset and all of its dependencies are promoted, production traffic is rerouted. The rerouting of traffic makes the on-premises assets obsolete, allowing them to be decommissioned.

The process of promotion varies according to the workload's architecture. However, there are several consistent prerequisites and a few common tasks. This article describes each and serves as a kind of pre-promotion checklist.

## Prerequisite processes

Each of the following processes should be executed, documented, and validated prior to production deployment:

- **Assess:** The workload has been assessed for cloud compatibility.
- **Architect:** The structure of the workload has been properly designed to align with the chosen cloud provider.
- **Replicate:** The assets have been replicated to the cloud environment.
- **Stage:** The replicated assets have been restored in a staged instance of the cloud environment.
- **Business testing:** The workload has been fully tested and validated by business users.
- **Business change plan:** The business has shared a plan for the changes to be made in accordance with the production promotion; this should include a user adoption plan, changes to business processes, users that require training, and timelines for various activities.
- **Ready:** Generally, a series of technical changes must be made before promotion.

## Best practices to execute prior to promotion

The following technical changes will likely need to be completed and documented as part of the promotion process:

- **Domain alignment.** Some corporate policies require separate domains for staging and production. Ensure that all assets are joined to the proper domain.
- **User routing.** Validate that users are accessing the workload through proper network routes; verify consistent performance expectations.
- **Identity alignment.** Validate that the users being rerouted to the application have proper permissions within the domain to host the application.
- **Performance.** Perform a final validation of workload performance to minimize surprises.
- **Validation of business continuity and disaster recovery.** Validate that proper backup and recovery processes are functioning as expected.
- **Data classification.** Validate data classification to ensure that proper protections and policies have been implemented.
- **Chief information security officer (CISO) verification.** Validate that the information security officer has reviewed the workload, business risks, risk tolerance, and mitigation strategies.

## Final step: Promote

Workloads will require varying levels of detailed review and promotion processes. However, network realignment serves as the common final step for all promotion releases. When everything else is ready, update DNS records or

IP addresses to route traffic to the migrated workload.

## Next steps

Promotion of a workload signals the completion of a release. However, in parallel with migration, retired assets need to be [decommissioned](#) taking them out of service.

[Decommission retired assets](#)

# Decommission retired assets

3/31/2020 • 2 minutes to read • [Edit Online](#)

After a workload is promoted to production, the assets that previously hosted the production workload are no longer required to support business operations. At that point, the older assets are considered retired. Retired assets can then be decommissioned, reducing operational costs. Decommissioning a resource can be as simple as turning off the power to the asset and disposing of the asset responsibly. Unfortunately, decommissioning resources can sometimes have undesired consequences. The following guidance can aid in properly decommissioning retired resources, with minimal business interruptions.

## Cost savings realization

When cost savings are the primary motivation for a migration, decommissioning is an important step. Until an asset is decommissioned, it continues to consume power, environmental support, and other resources that drive costs. After the asset is decommissioned, the costs savings can start to be realized.

## Continued monitoring

After a migrated workload is promoted, the assets to be retired should continue to be monitored to validate that no additional production traffic is being routed to the wrong assets.

## Testing windows and dependency validation

Even with the best planning, production workloads may still contain dependencies on assets that are presumed retired. In such cases, turning off a retired asset could cause unexpected system failures. As such, the termination of any assets should be treated with the same level of rigor as a system maintenance activity. Proper testing and outage windows should be established to facilitate the termination of the resource.

## Holding period and data validation

It's not uncommon for migrations to miss data during replication processes. This is especially true for older data that isn't used on a regular basis. After a retired asset has been turned off, it is still wise to maintain the asset for a while to serve as a temporary backup of the data. Companies should allow at least 30 days for holding and testing before destroying retired assets.

## Next steps

After retired assets are decommissioned, the migration is completed. This creates a good opportunity to improve the migration process, and a [retrospective](#) engages the cloud adoption team in a review of the release in an effort to learn and improve.

[Retrospective](#)

# How do retrospectives help build a growth mindset?

11/9/2020 • 2 minutes to read • [Edit Online](#)

"Culture eats strategy for breakfast." The best migration plan can easily be undone, if it doesn't have executive support and encouragement from leadership. Learning, growing, and even failure are at the heart of a growth mindset. They're also at the heart of any transformation effort.

Humility and curiosity are never more important than during a business transformation. Embracing digital transformation requires both in ample supply. These traits are strengthened by regular introspection and an environment of encouragement. When employees are encouraged to take risks, they find better solutions. When employees are allowed to fail and learn, they succeed. Retrospectives are an opportunity for such investigation and growth.

Retrospectives reinforce the principles of a growth mindset: experimentation, testing, learning, sharing, growing, and empowering. They provide a safe place for team members to share the challenges faced in the current sprint. And they allow the team to discuss and collaborate on ways to overcome those challenges. Retrospectives empower the team to create sustainable growth.

## Retrospective structure

A quick search on any search engine will offer many different approaches and tools for running a retrospective. Depending on the maturity of the culture and experience level of the team, these could prove useful. However, the general structure of a retrospective remains roughly the same. During these meetings, each member of the team is expected to contribute a thought regarding three basic questions:

- What went well?
- What could have been better?
- What did we learn?

Although these questions are simple in nature, they require employees to pause and reflect on their work over the last iteration. This small pause for introspection is the primary building block of a growth mindset. The humility and honesty produced when sharing the answers can become infectious beyond the time contract for the retrospective meeting.

## Leadership's role in a retrospective

The topic of leadership involvement in a retrospective is highly debated. Many technical teams suggest that leaders of any level should not be involved in the process, since it could discourage transparency and open dialogue. Others suggest that retrospectives are a good place for leaders to stay connected and to find ways to provide additional support. This decision is best left to the team and its leadership structure.

If leaders are involved in the retrospective, one role is highly encouraged. The leader's primary duty in a retrospective is to make the team feel safe. Creating a growth mindset within a culture requires employees to be free to share their failures and successes without fear of rebuke. Leaders who applaud the courage and humility required to admit shortcomings are more likely to see a growth mindset established in their teams. When leaders take action on data points shared in a retrospective, they're likely to see this tool become an ineffective formality.

## Lessons learned

Highly effective teams don't just run retrospective meetings. They live retrospective processes. The lessons learned and shared in these meetings can influence process, shape future work, and help the team execute more

effectively. Lessons learned in a retrospective should help the team grow organically. The primary byproducts of a retrospective are an increase in experimentation and a refinement of the lessons learned by the team.

That new growth is most tangibly represented in changes to the release or iteration backlog.

The retrospective marks the end of a release or iteration, as teams gain experience and learn lessons, and they adjust the [adjust the release and iteration backlog](#) to reflect new processes and experiments to be tested. This starts the next iteration through the migration processes.

# Skills readiness for cloud migration

11/9/2020 • 2 minutes to read • [Edit Online](#)

During a cloud migration, it is likely that employees, as well as some incumbent systems integration partners or managed services partners, will need to develop new skills to be effective during migration efforts.

There are four distinct processes that are completed iteratively in the Migrate methodology. The following sections align the necessary skills for each of those processes with references to two prerequisites for skilling resources.

## Prerequisites skilling resources

Implementation of the Migrate methodology builds on the skills acquired during the [Plan phase](#) and [Ready phase](#) of the migration journey.

## Assess skilling resources

The following tools can aid the team in execution of assess activities:

- [Balance the portfolio](#): Ensure balance and proper investment allocations across an application portfolio.
- [Build a business justification](#): Create and understand the business justification driving the cloud migration effort.
- [Rationalize the digital estate](#): Rationalize assets in the digital estate.
- [Application portfolio assessment](#): Criteria for making decisions regarding migration or innovation options within the application portfolio.
- [Assessing and planning Microsoft Azure migration](#): A Pluralsight course to aid in assessing on-premises workloads.

During assess processes, architects will design solutions for each workload. The following skilling resources help prepare architects for these tasks:

- [Foundations for cloud architecture](#): A Pluralsight course to help architect the right foundational solutions.
- [Microsoft Azure architecture: Getting started](#): A Pluralsight course to give architects a foundational knowledge in Azure architecture.
- [Designing migrations for Microsoft Azure](#): A Pluralsight course to help architects design a migration solution.

## Migrate skilling resources

The following tutorial can prepare the team for migration activities:

- [Migrate to Azure](#): Using Azure Migrate to migrate VMs to Azure.
- [Rehosting workloads to Azure](#): A Pluralsight course that teaches viewers how to rehost workloads to Azure.
- [Migrating physical and virtual servers to Azure](#): A Pluralsight course for migrating servers to Azure.
- [Import and export data to Azure](#): A Pluralsight course on the movement of data to and from Azure.

## Optimize and promote process changes

The following tools can help the team optimize resources and promote to production:

- [Cost and sizing](#): Adjust sizing to align costs and budgets.
- [Promote a workload](#): Change network configuration to reroute production users to migrated workloads.

## Secure and manage process changes

The following tools can help the team find ways to secure and manage migrated assets:

- [Secure and manage workloads in Azure](#): Best practices for securing and managing workloads in Azure.

## Next steps

Return to the [migration best practices checklist](#) to ensure your migration method is fully aligned.

[Migration best practices checklist](#)

# Cloud innovation in the Cloud Adoption Framework

11/9/2020 • 2 minutes to read • [Edit Online](#)

All IT portfolios contain a few workloads and ideas that could significantly improve a company's position in the market. Most cloud adoption efforts focus on the migration and modernization of existing workloads. It's innovation, however, that can provide the greatest business value. Cloud adoption-related innovation can unlock new technical skills and expanded business capabilities.

This section of the Cloud Adoption Framework focuses on the elements of your portfolio that drive the greatest return on investment.

To prepare you for this phase of the cloud adoption lifecycle, the framework suggests the following exercises:

1	<p><b>Business value consensus:</b> Before you decide on technical solutions, identify how new innovation can drive business value. Map that value to your cloud strategy. In this incremental methodology, business value is represented by a hypothesis about customer needs.</p>
2	<p><b>Azure innovation guide:</b> Azure includes cloud tools to accelerate the deployment of innovative solutions. Depending on your hypothesis, you might consider various combinations of tools. The creation of a minimum viable product (MVP) with basic tools is suggested.</p>
3	<p><b>Best practices:</b> Your architectural decisions should follow best practices for each tool in the toolchain. By adhering to such guidance, you can better accelerate solution development and provide a reference for solid architectural designs.</p>
4	<p><b>Feedback loops:</b> During each iteration, the solutions under development offer a way for your teams to learn alongside customers. Fast and accurate feedback loops with your customers can help you better test, measure, learn, and ultimately reduce the time to market impact. Learn how Azure and GitHub accelerate feedback loops.</p>

## Innovation summary

The [considerations overview](#) establishes a common language for innovation across application development, DevOps, IT, and business teams. The following approach builds on existing lean methodologies. It's designed to help you create a cloud-focused conversation about customer adoption and a scientific model for creating business value. The approach also maps existing Azure services to manageable decision processes. This alignment can help you find the right technical options to address specific customer needs or hypotheses.

## Innovate

## Start with customer adoption

### Build



Deliver on a hypothesis based on customer empathy.  
*Build a minimally viable product to meet a defined customer need.*

### Measure



Test the hypothesis based on customer observations.  
*Build a growth mindset by candidly testing assumptions.*

### Learn



Apply a growth mindset through continuous learning. *Iterate quickly to refine thinking; Turn fast fails into impactful change.*

## Then develop digital inventions



### Democratize data

Data in the hands of customers, partners, & employees drives innovative observation.  
*Ingest, integrate, categorize & share data.*



### Engage via apps

People connect with knowledge through apps & experiences.  
*Empower professional and citizen developers to create apps quickly.*



### Empower adoption

Encourage innovation by reducing friction to adoption & partnership.  
*Architect for visibility, collaboration, speed & feedback loops*



### Interact with devices

Digital & physical lines have blurred across multiple-channels.  
*Deliver experiences across devices, IoT, & mixed reality.*



### Predict & influence

Look to the future to lead innovation. *Look past current data to inform experiences, & interactions through predictive tools.*

## Suggested skills

Readiness for the new skills and responsibilities that come with cloud adoption doesn't come easily. Microsoft Learn provides a rewarding approach to hands-on learning that helps you achieve your goals faster. Earn points and levels, and achieve more!

Here are a couple of examples of role-specific learning paths on Microsoft Learn that align with the Innovate methodology of the Cloud Adoption Framework.

**Administer containers in Azure:** Azure Container Instances are the quickest and easiest way to run containers in Azure. This learning path will teach you how to create and manage your containers, and how you can use Azure Container Instances to provide elastic scale for Kubernetes.

**Create serverless applications:** Azure Functions enable the creation of event-driven, compute-on-demand systems that can be triggered by various external events. Learn to use functions to execute server-side logic and build serverless architectures.

To discover additional learning paths, browse the [Microsoft Learn catalog](#). Use the **Roles** filter to align learning paths with your role.

# Azure innovation guide overview

11/9/2020 • 2 minutes to read • [Edit Online](#)

## NOTE

This guide provides a starting point for innovation guidance in the Cloud Adoption Framework. It is also available in the [Azure Quickstart Center](#).

Before you start developing innovative solutions by using Azure services, you need to prepare your environment, which includes preparing to manage customer feedback loops. In this guide, we introduce features that help you engage customers, build solutions, and drive adoption. For more information, best practices, and considerations related to preparing your cloud environment, see the [Cloud Adoption Framework innovate section](#).

In this guide, you'll learn how to:

- **Manage customer feedback:** Set up tools and processes to manage the build-measure-learn feedback loop by using GitHub and Azure DevOps.
- **Democratize data:** Data alone might be enough to drive innovative solutions to your customers. Deploy common data options in Azure.
- **Engage via applications:** Some innovation requires an engaging experience. Use cloud-native application platforms to create engaging experiences.
- **Empower adoption:** Invention is great, but a plan to reduce friction is needed to empower and scale adoption. Deploy a foundation for CI/CD, DevOps, and other adoption enablers.
- **Interact through devices:** Create ambient experiences to bring your applications and data closer to the customers' point of need. IoT, mixed reality, and mobile experiences are easier with Azure.
- **Predict and influence:** Find patterns in data. Put those patterns to work to predict and influence customer behaviors by using Azure-based predictive analytics tools.

## TIP

For an interactive experience, view this guide in the Azure portal. Go to the [Azure Quickstart Center](#) in the Azure portal, select [Azure innovation guide](#), and then follow the step-by-step instructions.

## Next steps:

- [Prepare for innovation with a shared repository and ideation management tools](#)

This guide provides interactive steps that let you try features as they're introduced. To come back to where you left off, use the breadcrumb for navigation.

# Prepare for customer feedback

11/9/2020 • 3 minutes to read • [Edit Online](#)

User adoption, engagement, and retention are key to successful innovation. Why?

Building an innovative new solution isn't about giving users what they want or think they want. It's about the formulation of a hypothesis that can be tested and improved upon. That testing comes in two forms:

- **Quantitative (testing feedback):** This feedback measures the actions we hope to see.
- **Qualitative (customer feedback):** This feedback tells us what those metrics mean in the customer's voice.

Before you integrate feedback loops, you need to have a shared repository for your solution. A centralized repo will provide a way to record and act on all the feedback coming in about your project. [GitHub](#) is the home for open source software. It's also one of the most commonly used platforms for hosting source code repositories for commercially developed applications. The article on [building GitHub repositories](#) can help you get started with your repo.

Each of the following tools in Azure integrates with (or is compatible with) projects hosted in GitHub:

- [Quantitative feedback for web apps](#)
- [Quantitative feedback for APIs](#)
- [Qualitative feedback](#)
- [Close the loop with pipelines](#)

Application Insights is a monitoring tool that provides near-real-time quantitative feedback on the usage of your application. This feedback can help you test and validate your current hypothesis to shape the next feature or user story in your backlog.

## Action

To view quantitative data on your applications:

1. Go to [Application Insights](#).
  - If your application doesn't appear in the list, select **add** and follow the prompts to start configuring Application Insights.
  - If the desired application is in the list, select it.
2. The [overview](#) pane includes some statistics on the application. Select [application dashboard](#) to build a custom dashboard for data that's more relevant to your hypothesis.

GO TO APPLICATION  
INSIGHTS

To view the data about your applications, go to the [Azure portal](#).

## Learn more

- [Set up Azure Monitor](#)
- [Get started with Azure Monitor Application Insights](#)
- [Build a telemetry dashboard](#)

# Democratize data

11/9/2020 • 2 minutes to read • [Edit Online](#)

One of the first steps in democratizing data is to enhance data discoverability. Cataloging and managing data sharing can help enterprises get the most value from their existing information assets. A data catalog makes data sources easy to discover and understand by the users who manage the data. Azure Data Catalog enables management inside an enterprise, whereas Azure Data Share enables management and sharing outside the enterprise.

Azure services that provide data processing, like Azure Time Series Insights and Stream Analytics, are other capabilities that customers and partners are successfully using for their innovation needs.

- [Catalog](#)
- [Share](#)
- [Insights](#)

## Azure Data Catalog

Azure Data Catalog addresses the discovery challenges of data consumers and enables data producers who maintain information assets. It bridges the gap between IT and the business, allowing everyone to contribute their insights. You can store your data where you want it and connect with the tools you want to use. With Azure Data Catalog, you can control who can discover registered data assets. You can integrate into existing tools and processes by using open REST APIs.

- Register
- Search and annotate
- Connect and manage

[Go to the Azure Data Catalog documentation](#)

## Action

You can use only one Azure Data Catalog per organization. If a catalog has already been created for your organization, you can't add more catalogs.

To create a catalog for your organization:

1. Go to **Azure Data Catalog**.
2. Select **Create**.

GO TO AZURE DATA  
CATALOG

# Engage customers through applications

11/9/2020 • 9 minutes to read • [Edit Online](#)

Innovation with applications includes both modernizing your existing applications that are hosted on-premises and building cloud-native applications by using containers or serverless technologies. Azure provides PaaS services like Azure App Service to help you easily modernize your existing web and API apps written in .NET, .NET Core, Java, Node.js, Ruby, Python, or PHP for deployment in Azure.

With an open-standard container model, building microservices or containerizing your existing applications and deploying them on Azure is simple when you use managed services like Azure Kubernetes Service, Azure Container Instances, and Web App for Containers. Serverless technologies like Azure Functions and Azure Logic Apps use a consumption model (pay for what you use) and help you focus on building your application rather than deploying and managing infrastructure.

- [Deliver value faster](#)
- [Create cloud-native applications](#)
- [Isolate points of failure](#)

One of the advantages of cloud-based solutions is the ability to gather feedback faster and start delivering value to your user. Whether that user is an external customer or a user in your own company, the faster you can get feedback on your applications, the better.

## Azure App Service

Azure App Service provides a hosting environment for your applications that removes the burden of infrastructure management and OS patching. It provides automation of scale to meet the demands of your users while bound by limits that you define to keep costs in check.

Azure App Service provides first-class support for languages like ASP.NET, ASP.NET Core, Java, Ruby, Node.js, PHP, and Python. If you need to host another runtime stack, Web App for Containers lets you quickly and easily host a Docker container within App Service, so you can host your custom code stack in an environment that gets you out of the server business.

### Action

To configure or monitor Azure App Service deployments:

1. Go to **App Services**.
2. Configure a new service: select **Add** and follow the prompts.
3. Manage existing services: select the desired application from the list of hosted applications.

GO TO APP  
SERVICES

## Azure Cognitive Services

With Azure Cognitive Services, you can infuse advanced intelligence directly into your application through a set of APIs that let you take advantage of Microsoft-supported AI and machine learning algorithms.

### Action

To configure or monitor Azure Cognitive Services deployments:

1. Go to **Cognitive Services**.
2. Configure a new service: select **Add** and follow the prompts.
3. Manage existing services: select the desired service from the list of hosted services.

GO TO COGNITIVE  
SERVICES

## Azure Bot Service

Azure Bot Service extends your standard application by adding a natural bot interface that uses AI and machine learning to create a new way to interact with your customers.

### Action

To configure or monitor Azure Bot Service deployments:

1. Go to **Bot Services**.
2. Configure a new service: select **Add** and follow the prompts.
3. Manage existing services: select the desired bot from the list of hosted services.

GO TO BOT  
SERVICES

## Azure DevOps

During your innovation journey, you'll eventually find yourself on the path to DevOps. Microsoft has long had an on-premises product known as Team Foundation Server (TFS). During our own innovation journey, Microsoft developed Azure DevOps, a cloud-based service that provides build and release tools supporting many languages and destinations for your releases. For more information, see [Azure DevOps](#).

## Visual Studio App Center

As mobile apps continue to grow in popularity, the need for a platform that can provide automated testing on real devices of various configurations grows. Visual Studio App Center not only provides a place where you can test your applications across iOS, Android, Windows, and macOS, it also provides a monitoring platform that can use Azure Application Insights to analyze your telemetry quickly and easily. For more information, see [Visual Studio App Center](#).

Visual Studio App Center also provides a notification service that lets you use a single call to send notifications to your application across platforms without having to contact each notification service individually. For more information, see [Visual Studio App Center Push \(ACP\)](#).

### Learn more

- [App Service overview](#)
- [Web App for Containers: Run a custom container](#)
- [Introduction to Azure Functions](#)
- [Azure for .NET and .NET Core developers](#)
- [Azure SDK for Python documentation](#)
- [Azure for Java cloud developers](#)
- [Create a PHP web app in Azure](#)
- [Azure SDK for JavaScript documentation](#)
- [Azure SDK for Go documentation](#)
- [DevOps solutions](#)

# Empower adoption

11/9/2020 • 7 minutes to read • [Edit Online](#)

You know that innovation is critical to business success. You don't accomplish innovation solely through the introduction of new technologies. You need to focus on supporting the people who catalyze change and create the new value that you seek. Developers are at the center of digital transformation, and to empower them to achieve more, you need to accelerate developer velocity. To unleash the creative energy of developer teams, you need to help them build productively, foster global and secure collaboration, and remove barriers so they can scale innovation.

## Generate value

- In every industry, every organization is trying to do one thing: drive constant value generation.
- The focus on innovation is essentially a process to help your organization find new ways to generate value.
- Perhaps the biggest mistake organizations make is trying to create new value by introducing new technologies.
- Sometimes the attitude is "if we just use more technology, we'll see things improve." But innovation is first and foremost a people story.
- Innovation is about the combination of people and technology.

Organizations that successfully innovate see vision, strategy, culture, unique potential, and capabilities as the foundational elements. They then turn to technology with a specific purpose in mind. Every company is becoming a software company. The hiring of software engineers is growing at a faster rate outside the tech industry than inside, according to LinkedIn data.

Innovation is accomplished when organizations support their people to create the value they seek. One group of those people, developers, is a catalyst for innovation. They play an increasingly vital role in value creation and growth across every industry. They're the builders of our era, writing the world's code and sitting at the heart of innovation. Innovative organizations build a culture that empowers developers to achieve more.

- [Developer productivity](#)
- [Innovate collaboratively](#)
- [Innovation characteristics](#)
- [LiveOps innovation](#)

## Developer velocity

Empowering developers to invent means accelerating developer velocity, enabling them to create more, innovate more, and solve more problems. Developer velocity is the underpinning of each organization's tech intensity. Developer velocity isn't just about speed. It's also about unleashing developer ingenuity, turning your developers' ideas into software with speed and agility so that innovative solutions can be built. The differentiated Azure solution is uniquely positioned to unleash innovation in your organization.

## Build productively

There are several areas of opportunity where Azure can help you build productively:

- Ensure developers become and stay proficient in their domain by helping them advance their knowledge.
- Hone the right skills by giving them the right tools.

One of the best ways to improve your developers' skills is by giving them tools they know and love. Azure tools meet developers where they are today and introduce them to new technologies in the context of the code they're writing. With the Azure commitment to open-source software and support for all languages and frameworks in

Azure tools, your developers can build how they want and deploy where you want.

Azure DevOps provides best-in-class tools for every developer. Azure developer services infuse modern development practices and emerging trends into our tools. With the Azure platform, developers have access to the latest technologies and a cutting-edge toolchain that supports the way they work.

- AI-assisted development tools
- Integrated tools and cloud
- Remote development and pair programming

[Go to Azure DevOps documentation](#)

#### Action

To create a DevOps project:

1. Go to [Azure DevOps Projects](#).
2. Select **Create DevOps project**.
3. Select **Runtime, Framework, and Service**.

GO TO AZURE DEVOPS  
PROJECTS

# Interact through devices

11/9/2020 • 5 minutes to read • [Edit Online](#)

Innovate through intermittently connected and perceptive edge devices. Orchestrate millions of such devices, acquire and process limitless data, and take advantage of a growing number of multisensory, multidevice experiences. For devices at the edge of your network, Azure provides a framework for building immersive and effective business solutions. With ubiquitous computing, enabled by Azure combined with AI technology, you can build every type of intelligent application and system you can envision.

Azure customers employ a continually expanding set of connected systems and devices that gather and analyze data (close to their users, the data, or both). Users get real-time insights and experiences, delivered by highly responsive and contextually aware applications. By moving parts of the workload to the edge, these devices can spend less time sending messages to the cloud and react more quickly to spatial events.

- Industrial assets
- [Microsoft HoloLens 2](#)
- [Azure Sphere](#)
- [Azure Kinect DK](#)
- Drones
- [Azure SQL Edge](#)
- [IoT plug and play](#)
- [Global scale IoT service](#)
- [Azure Digital Twins](#)
- [Location intelligence](#)
- [Spatial experiences](#)
- [Azure Remote Rendering](#)

Architect solutions that exercise bidirectional communication with IoT devices at billions scale. Use out-of-box, device-to-cloud telemetry data to understand the state of your devices and define message routes to other Azure services just through configuration. By taking advantage of cloud-to-device messages, you can reliably send commands and notifications to your connected devices and track message delivery with acknowledgment receipts. And you'll automatically resend device messages as needed to accommodate intermittent connectivity.

Here are a few features you'll find:

- **Security-enhanced communication** channel for sending and receiving data from IoT devices.
- **Built-in device management** and provisioning to connect and manage IoT devices at scale.
- **Full integration with Event Grid** and serverless compute, simplifying IoT application development.
- **Compatibility with Azure IoT Edge** for building hybrid IoT applications.

## Learn more

- [Azure IoT Hub](#)
- [Azure IoT Hub Device Provisioning Service \(DPS\)](#)

## Action

To create an IoT hub:

1. Go to [IoT Hub](#).
2. Select [Create IoT hub](#).

GO TO IOT  
HUB

The Azure IoT Hub Device Provisioning Service is a helper service for Azure IoT Hub that enables zero-touch, just-in-time provisioning.

## Action

To create an Azure IoT Hub Device Provisioning Service:

1. Go to **Device Provisioning Services**.
2. Select **Add**.

GO TO DEVICE PROVISIONING  
SERVICES

# Innovate with AI

11/9/2020 • 3 minutes to read • [Edit Online](#)

As an innovator, your company has rich information about its business and its customers. Using AI, your company can:

- Make predictions about customer needs.
- Automate business processes.
- Discover information that's latent in unstructured data.
- Engage with customers in new ways to deliver better experiences.

This article introduces a few approaches to innovating with AI. The following table can help you find the best solution for your implementation needs.

SOLUTION CATEGORY	DESCRIPTION	REQUIRED SKILLS
Machine learning	<b>Azure Machine Learning</b> Build, deploy, and manage your own machine learning models.	Data scientist and developer
AI applications and agents	<b>Azure Cognitive Services</b> Use domain-specific AI models for vision, speech, language, and decision that can be customized with your data.  <b>Azure Bot Service</b> Improve customer engagement by adding bots to your applications and websites.	Developer
Knowledge mining	<b>Azure Cognitive Search</b> Uncover insights that are latent in your content, including documents, contracts, images, and other data types.	Developer

## Machine learning

Azure provides advanced machine learning capabilities. Build, train, and deploy your machine learning models across the cloud and edge by using Azure Machine Learning. Develop models faster by using automated machine learning. Use tools and frameworks of your choice without being locked in.

For more information, see [Azure Machine Learning overview](#) and [getting started with your first machine learning experiment](#). For more information on the open source model format and runtime for machine learning, see [ONNX Runtime](#).

### Action

A data scientist can use Azure Machine Learning to train and build a model by using advanced languages such as Python and R, as well as by using a drag-and-drop visual experience. To get started with Azure Machine Learning:

1. In the Azure portal, search for and select **Machine Learning**.
2. Select **Add**, and follow the steps in the portal to create a workspace.

3. The new workspace provides both low-code and code-driven approaches for data scientists to train, build, deploy, and manage models.

GO TO AZURE MACHINE LEARNING

RESOURCES

Go directly to Azure Machine Learning resources in the [Azure portal](#).

## AI applications and agents

Azure provides a set of pre-built AI services called Cognitive Services to build AI applications. Additionally, Azure offers bot service, which allows developers to build conversational AI agents that improve customer and employee engagement.

### AI applications

Cognitive Services enables you to incorporate the AI capabilities of vision, speech, language, and decision into your applications. Most predictive models don't require additional training. These services are useful when you don't have data scientists on staff to train the predictive model. Other services require minimal training.

For more information about the training that might be required and a list of available services across vision, speech, language, and decision-making, see the [Cognitive Services](#) documentation.

#### Action

To get started with a Cognitive Services API:

1. In the Azure portal, search for and select **Cognitive Services**.
2. Select **Add** to find a Cognitive Services API in Azure Marketplace.
3. Search for and select a service:
  - If you know the name of the service you want to use, enter the name in **Search the Marketplace**. Then select the service.
  - For a list of Cognitive Services APIs, next to the **Cognitive Services** heading, select **see more**. Then select the service.
4. Select **Create**, and follow the steps in the portal to provision the service.

GO TO COGNITIVE

SERVICES

Go directly to Cognitive Services in the [Azure portal](#).

### AI agents

Interact more naturally with your customers and improve customer engagement through conversational experiences powered by Bot Framework and Azure Bot Service. In addition, use Cognitive Services APIs like Language Understanding (LUIS), QnA Maker, and Speech service. These help your customers with common tasks, leaving your call center agents time to focus on more nuanced, higher value cases.

For more information on how to build bots, see [Azure Bot Service](#).

#### Action

To get started with Azure Bot Service:

1. In the Azure portal, search for and select **Bot Services**.
2. Select **Add**, and then select **web app bot** or **bot channels registration**.
3. Select **Create**. Then follow the steps in the portal to provision the service.

GO TO AZURE BOT  
SERVICE

Go directly to Azure Bot Service in the [Azure portal](#).

## Knowledge mining

Use Azure Cognitive Search to uncover latent insights from your content, including documents, images, and media. You can discover patterns and relationships in your content, understand sentiment, and extract key phrases.

Azure Cognitive Search uses the same natural language stack that Bing and Microsoft Office use. Spend more time innovating and less time maintaining a complex cloud search solution.

For more information, see [What is Azure Cognitive Search?](#)

### Action

To get started:

1. In the Azure portal, search for and select **Azure Cognitive Search**.
2. Follow the steps in the portal to provision the service.

GO TO AZURE COGNITIVE  
SEARCH

Go directly to Azure Cognitive Search in the [Azure portal](#).

---

# Kubernetes in the Cloud Adoption Framework

11/9/2020 • 2 minutes to read • [Edit Online](#)

Review a prescriptive framework that includes the tools, programs, and content (best practices, configuration templates, and architecture guidance) to simplify adoption of Kubernetes and cloud-native practices at scale.

The list of required actions is categorized by persona to drive a successful deployment of applications on Kubernetes, from proof of concept to production, then scaling and optimization.

## Get started

To prepare for this phase of the cloud adoption lifecycle, use the following exercises:

- [Application development and deployment](#): Examine patterns and practices of application development, configure CI/CD pipelines, and implement site reliability engineering (SRE) best practices.
- [Cluster design and operations](#): Identify for cluster configuration and network design. Ensure future scalability by automating infrastructure provisioning. Maintain high availability by planning for business continuity and disaster recovery.
- [Cluster and application security](#): Familiarize yourself with Kubernetes security essentials. Review the secure setup for clusters and application security guidance.

# Application development and deployment

11/9/2020 • 4 minutes to read • [Edit Online](#)

Examine patterns and practices of application development, configure Azure Pipelines, and implement site reliability engineering (SRE) best practices.

## Plan, train, and proof

As you get started, the checklist and resources below will help you plan your application development and deployment. You should be able to answer these questions:

- Have you prepared your development environment and setup workflow?
- How will you structure the project folder to support Kubernetes application development?
- Have you identified state, configuration, and storage requirements of your application?

CHECKLIST	RESOURCES
<b>Prepare your development environment.</b> Configure your environment with the tools you need to create containers and set up your development workflow.	<a href="#">Working with Docker in Visual Studio Code</a> <a href="#">Working with Kubernetes in Visual Studio Code</a> <a href="#">Introduction to Azure Dev Spaces</a>
<b>Containerize your application.</b> Familiarize yourself with the end-to-end Kubernetes development experience, including application scaffolding, inner-loop workflows, application-management frameworks, CI/CD pipelines, log aggregation, monitoring, and application metrics.	<a href="#">Containerize your applications with Docker and Kubernetes (e-book)</a> <a href="#">End-to-end Kubernetes development experience on Azure (webinar)</a>
<b>Review common Kubernetes scenarios.</b> Kubernetes is often thought of as a platform for delivering microservices, but it's becoming a much broader platform. Watch this video to learn about common Kubernetes scenarios such as batch analytics and workflow.	<a href="#">Common scenarios to use Kubernetes (video)</a>
<b>Prepare your application for Kubernetes.</b> Prepare your application file system layout for Kubernetes and organize for weekly or daily releases. Learn how the Kubernetes deployment process enables reliable, zero-downtime upgrades.	<a href="#">Project design and layout for successful Kubernetes applications (webinar)</a> <a href="#">How Kubernetes deployments work (video)</a> <a href="#">Go through an AKS workshop</a>
<b>Manage application storage.</b> Understand the performance needs and access methods for pods so that you can provide the appropriate storage options. You should also plan for ways to back up and test the restore process for attached storage.	<a href="#">The basics of stateful applications in Kubernetes (video)</a> <a href="#">State and data in Docker applications</a> <a href="#">Storage options in Azure Kubernetes Service</a>
<b>Manage application secrets.</b> Don't store credentials in your application code. A key vault should be used to store and retrieve keys and credentials.	<a href="#">How Kubernetes and configuration management work (video)</a> <a href="#">Understand secrets management in Kubernetes (video)</a> <a href="#">Using Azure Key Vault with Kubernetes</a> <a href="#">Use Azure AD pod identity to authenticate and access Azure resources</a>

## Deploy to production and apply best practices

As you prepare the application for production, you should implement a minimum set of best practices. Use the checklist below at this stage. You should be able to answer these questions:

- Can you monitor all aspects of your application?
- Have you defined resource requirements for your application? How about scaling requirements?
- Can you deploy new versions of the application without affecting production systems?

CHECKLIST	RESOURCES
<b>Configure readiness and liveness health checks.</b> Kubernetes uses readiness and liveness checks to know when your application is ready to receive traffic and when it needs to be restarted. Without defining such checks, Kubernetes will not be able to determine if your application is up and running.	<a href="#">Liveness and readiness checks</a>
<b>Configure logging, application monitoring, and alerting.</b> Monitoring your containers is critical, especially when you're running a production cluster, at scale, with multiple applications. The recommended logging method for containerized applications is writing to the standard output (stdout) and standard error (stderr) streams.	<a href="#">Logging in Kubernetes</a> <a href="#">Get started with monitoring and alerting for Kubernetes (video)</a> <a href="#">Azure Monitor for containers</a> <a href="#">Enable and review Kubernetes master node logs in Azure Kubernetes Service (AKS)</a> <a href="#">View Kubernetes logs, events, and pod metrics in real time</a>
<b>Define resource requirements for the application.</b> A primary way to manage the compute resources within a Kubernetes cluster is using pod requests and limits. These requests and limits tell the Kubernetes scheduler what compute resources a pod should be assigned.	<a href="#">Define pod resource requests and limits</a>
<b>Configure application scaling requirements.</b> Kubernetes supports horizontal pod autoscaling to adjust the number of pods in a deployment depending on CPU utilization or other select metrics. To use the autoscaler, all containers in your pods must have CPU requests and limits defined.	<a href="#">Configure horizontal pod autoscaling</a>
<b>Deploy applications using an automated pipeline and DevOps.</b> The full automation of all steps between code commit to production deployment allows teams to focus on building code and removes the overhead and potential human error in manual mundane steps. Deploying new code is quicker and less risky, helping teams become more agile, more productive, and more confident about their running code.	<a href="#">Evolve your DevOps practices</a> <a href="#">Setting up a Kubernetes build pipeline (video)</a> <a href="#">Deployment Center for Azure Kubernetes Service</a> <a href="#">GitHub Actions for deploying to Azure Kubernetes Service</a> <a href="#">CI/CD to Azure Kubernetes Service with Jenkins</a>

## Optimize and scale

Now that the application is in production, how can you optimize your workflow and prepare your application and team to scale? Use the optimization and scaling checklist to prepare. You should be able to answer these questions:

- Are cross-cutting application concerns abstracted from your application?
- Are you able to maintain system and application reliability, while still iterating on new features and versions?

CHECKLIST	RESOURCES
<p><b>Deploy an API gateway.</b> An API gateway serves as an entry point to microservices, decouples clients from your microservices, adds an additional layer of security, and decreases the complexity of your microservices by removing the burden of handling cross-cutting concerns.</p>	<a href="#">Use Azure API Management with microservices deployed in Azure Kubernetes Service</a>
<p><b>Deploy a service mesh.</b> A service mesh provides capabilities like traffic management, resiliency, policy, security, strong identity, and observability to your workloads. Your application is decoupled from these operational capabilities and the service mesh moves them out of the application layer and down to the infrastructure layer.</p>	<a href="#">How service meshes work in Kubernetes (video)</a> <a href="#">Learn about service meshes</a> <a href="#">Use Istio with Azure Kubernetes Service</a> <a href="#">Use Linkerd with Azure Kubernetes Service</a> <a href="#">Use Consul with Azure Kubernetes Service</a>
<p><b>Implement site reliability engineering (SRE) practices.</b> Site reliability engineering (SRE) is a proven approach to maintain crucial system and application reliability while iterating at the speed demanded by the marketplace.</p>	<a href="#">Introduction to site reliability engineering (SRE)</a> <a href="#">DevOps at Microsoft: Game streaming SRE</a>

# Cluster design and operations

11/9/2020 • 3 minutes to read • [Edit Online](#)

Identify for cluster configuration and network design. Future-proof scalability by automating infrastructure provisioning. Maintain high availability by planning for business continuity and disaster recovery.

## Plan, train, and proof

As you get started, the checklist and resources below will help you plan the cluster design. You should be able to answer these questions:

- Have you identified the networking design requirements for your cluster?
- Do you have workloads with varying requirements? How many node pools are you going to use?

CHECKLIST	RESOURCES
<p><b>Identify network design considerations.</b> Understand cluster network design considerations, compare network models, and choose the Kubernetes networking plug-in that fits your needs. For the Azure container networking interface (CNI), consider the number of IP addresses required as a multiple of the maximum pods per node (default of 30) and number of nodes. Add one node required during upgrade. When choosing load balancer services, consider using an ingress controller when there are too many services to reduce the number of exposed endpoints. For Azure CNI, the service CIDR has to be unique across the virtual network and all connected virtual networks to ensure appropriate routing.</p>	<ul style="list-style-type: none"><li>• <a href="#">Kubenet and Azure Container Networking Interface (CNI)</a></li><li>• <a href="#">Use kubenet networking with your own IP address ranges in Azure Kubernetes Service (AKS)</a></li><li>• <a href="#">Configure Azure CNI networking in Azure Kubernetes Service (AKS)</a></li><li>• <a href="#">Secure network design for an AKS cluster</a></li></ul>
<p><b>Create multiple node pools.</b> To support applications that have different compute or storage demands, you can optionally configure your cluster with multiple node pools. For example, use additional node pools to provide GPUs for compute-intensive applications or access to high-performance SSD storage.</p>	<ul style="list-style-type: none"><li>• <a href="#">Create and manage multiple node pools for a cluster in Azure Kubernetes Service</a></li></ul>
<p><b>Decide on availability requirements.</b> A minimum of two pods behind Azure Kubernetes Service ensures high availability of your application in case of pod failures or restarts. Use three or more pods to handle load during pod failures and restarts. For the cluster configuration, a minimum of 2 nodes in an availability set or virtual machine scale set is required to meet the service-level agreement of 99.95%. Use at least three pods to ensure pod scheduling during node failures and reboots. To provide a higher level of availability to your applications, clusters can be distributed across availability zones. These zones are physically separate datacenters within a given region. When the cluster components are distributed across multiple zones, your cluster is able to tolerate a failure in one of those zones. Your applications and management operations remain available even if an entire datacenter experiences an outage.</p>	<ul style="list-style-type: none"><li>• <a href="#">Create an Azure Kubernetes Service (AKS) cluster that uses availability zones</a></li></ul>

Go to production and apply best practices

As you prepare the application for production, you should implement a minimum set of best practices. Use the checklist below at this stage. You should be able to answer these questions:

- Are you able to confidently redeploy the cluster infrastructure?
- Have you applied resource quotas?

CHECKLIST	RESOURCES
<b>Automate cluster provisioning.</b> With infrastructure as code, you can automate infrastructure provisioning to provide more resiliency during disasters and gain agility to quickly redeploy the infrastructure as needed.	<ul style="list-style-type: none"><li>• <a href="#">Create a Kubernetes cluster with Azure Kubernetes Service using Terraform</a></li></ul>
<b>Plan for availability using pod disruption budgets.</b> To maintain the availability of applications, define pod disruption budgets (PDBs) to ensure that a minimum number of pods are available in the cluster during hardware failures or cluster upgrades.	<ul style="list-style-type: none"><li>• <a href="#">Plan for availability using pod disruption budgets</a></li></ul>
<b>Enforce resource quotas on namespaces.</b> Plan and apply resource quotas at the namespace level. Quotas can be set on compute resources, storage resources, and object count.	<ul style="list-style-type: none"><li>• <a href="#">Enforce resource quotas</a></li></ul>

## Optimize and scale

Now that the application is in production, how can you optimize your workflow and prepare your application and team to scale? Use the optimization and scaling checklist to prepare. You should be able to answer these questions:

- Do you have a plan for business continuity and disaster recovery?
- Can your cluster scale to meet application demands?
- Are you able to monitor your cluster and application health and receive alerts?

CHECKLIST	RESOURCES
<b>Automatically scale a cluster to meet application demands.</b> To keep up with application demands, you may need to adjust the number of nodes that run your workloads automatically using the cluster autoscaler.	<ul style="list-style-type: none"><li>• <a href="#">Configure Kubernetes cluster autoscaler</a></li></ul>
<b>Plan for business continuity and disaster recovery.</b> Plan for multiregion deployment, create a storage migration plan, and enable geo-replication for container images.	<ul style="list-style-type: none"><li>• <a href="#">Best practices for region deployments</a></li><li>• <a href="#">Azure Container Registry geo-replication</a></li></ul>
<b>Configure monitoring and troubleshooting at scale.</b> Set up alerting and monitoring for applications in Kubernetes. Learn about the default configuration, how to integrate more advanced metrics, and how to add your own custom monitoring and alerting to reliably operate your application.	<ul style="list-style-type: none"><li>• <a href="#">Get started with monitoring and alerting for Kubernetes (video)</a></li><li>• <a href="#">Configure alerts using Azure Monitor for containers</a></li><li>• <a href="#">Review diagnostic logs for master components</a></li><li>• <a href="#">Azure Kubernetes Service (AKS) diagnostics</a></li></ul>

# Cluster and application security

11/9/2020 • 3 minutes to read • [Edit Online](#)

Familiarize yourself with Kubernetes security essentials and review the secure setup for clusters and application security guidance.

## Plan, train, and proof

As you get started, the checklist and resources below will help you plan for cluster operations and security. You should be able answer these questions:

- Have you reviewed the security and threat model of Kubernetes clusters?
- Is your cluster enabled for role-based access control?

CHECKLIST	RESOURCES
<p><b>Familiarize yourself with the security essentials white paper.</b> The primary goals of a secure Kubernetes environment are ensuring that the applications it runs are protected, that security issues can be identified and addressed quickly, and that future similar issues will be prevented.</p>	<p><a href="#">The definitive guide to securing Kubernetes (white paper)</a></p>
<p><b>Review the security hardening setup for the cluster nodes.</b> A security hardened host OS reduces the surface area of attack and allows deploying containers securely.</p>	<p><a href="#">Security hardening in AKS virtual machine hosts</a></p>
<p><b>Setup cluster role-based access control (RBAC).</b> This control mechanism lets you assign users, or groups of users, permission to do things like create or modify resources, or view logs from running application workloads.</p>	<p><a href="#">Understand role-based access control (RBAC) in Kubernetes (video)</a> <a href="#">Integrate Azure AD with Azure Kubernetes Service</a> <a href="#">Limit access to cluster configuration file</a></p>

## Deploy to production and apply best practices

As you prepare the application for production, you should implement a minimum set of best practices. Use the checklist below at this stage. You should be able to answer these questions:

- Have you configured network security rules for ingress, egress, and intra-pod communication?
- Is your cluster configured to automatically apply node security updates?
- Are you running a security scanning solution for your cluster and container workloads?

CHECKLIST	RESOURCES
<p><b>Control access to clusters using group membership.</b> Configure Kubernetes role-based access control (RBAC) to limit access to cluster resources based on user identity or group membership.</p>	<p><a href="#">Control access to clusters using RBAC and Azure AD groups</a></p>
<p><b>Create a secrets management policy.</b> Securely deploy and manage sensitive information, such as passwords and certificates, using secrets management in Kubernetes.</p>	<p><a href="#">Understand secrets management in Kubernetes (video)</a></p>

CHECKLIST	RESOURCES
<b>Secure intra-pod network traffic with network policies.</b> Apply the principle of least privilege to control network traffic flow between pods in the cluster.	<a href="#">Secure intra-pod traffic with network policies</a>
<b>Restrict access to the API server using authorized IPs.</b> Improve cluster security and minimize attack surface by limiting access to the API server to a limited set of IP address ranges.	<a href="#">Secure access to the API server</a>
<b>Restrict cluster egress traffic.</b> Learn what ports and addresses to allow if you restrict egress traffic for the cluster. You can use Azure Firewall or a third-party firewall appliance to secure your egress traffic and define these required ports and addresses.	<a href="#">Control egress traffic for cluster nodes in AKS</a>
<b>Secure traffic with Web Application Firewall (WAF).</b> Use Azure Application Gateway as an ingress controller for Kubernetes clusters.	<a href="#">Configure Azure Application Gateway as an ingress controller</a>
<b>Apply security and kernel updates to worker nodes.</b> Understand the AKS node update experience. To protect your clusters, security updates are automatically applied to Linux nodes in AKS. These updates include OS security fixes or kernel updates. Some of these updates require a node reboot to complete the process.	<a href="#">Use kured to automatically reboot nodes to apply updates</a>
<b>Configure a container and cluster scanning solution.</b> Scan containers pushed into Azure Container Registry and gain deeper visibility to your cluster nodes, cloud traffic, and security controls.	<a href="#">Azure Container Registry integration with Security Center</a> <a href="#">Azure Kubernetes Service integration with Security Center</a>

## Optimize and scale

Now that the application is in production, how can you optimize your workflow and prepare your application and team to scale? Use the optimization and scaling checklist to prepare. You should be able to answer:

- Can you enforce governance and cluster policies at scale?

CHECKLIST	RESOURCES
<b>Enforce cluster governance policies.</b> Apply at-scale enforcements and safeguards on your clusters in a centralized, consistent manner.	<a href="#">Control deployments with Azure Policy</a>
<b>Rotate cluster certificates periodically.</b> Kubernetes uses certificates for authentication with many of its components. You may want to periodically rotate those certificates for security or policy reasons.	<a href="#">Rotate certificates in Azure Kubernetes Service (AKS)</a>

# AI in the Cloud Adoption Framework

11/9/2020 • 2 minutes to read • [Edit Online](#)

Review a prescriptive framework that includes the tools, programs, and content (best practices, configuration templates, and architecture guidance) to simplify adoption of AI and cloud-native practices at scale.

The list of required actions is categorized by persona to drive a successful deployment of AI in applications, from proof of concept to production, then scaling and optimization.

## Get started

To prepare for this phase of the cloud adoption lifecycle, use the following exercises:

- [Machine Learning model development, deployment, and management](#): Examine patterns and practices of building your own machine learning models, including MLOps, automated machine learning (AutoML), and Responsible ML learning tools such as InterpretML and FairLearn.
- [Adding domain-specific AI models to your applications](#): Learn about best practices for adding AI capabilities into your applications with Cognitive Services. Also learn about the key scenarios these services help you address.
- [Build your own conversational AI solution](#): Learn how to build your own Virtual Assistant, a conversational AI application that can understand language and speech, perceive vast amounts of information, and respond intelligently.
- [Build AI-driven knowledge mining solutions](#): Learn how to use knowledge mining to extract structured data from your unstructured content and discover actionable information across your organization's data.

# Machine learning

11/9/2020 • 2 minutes to read • [Edit Online](#)

Azure empowers you with the most advanced machine learning capabilities. Quickly and easily build, train, and deploy your machine learning models by using Azure Machine Learning. Machine Learning can be used for any kind of machine learning, from classical to deep, supervised, and unsupervised learning. Whether you prefer to write Python or R code, or use zero-code or low-code options such as the [designer](#), you can build, train, and track highly accurate machine learning and deep learning models in a Machine Learning workspace.

You can even start training on your local machine and then scale out to the cloud. The service also interoperates with popular deep learning and reinforcement open-source tools such as PyTorch, TensorFlow, scikit-learn, and Ray and RLlib.

Get started with [Machine Learning](#). You'll find a tutorial on how to get [started with your first machine learning experiment](#). To learn more about the open-source model format and runtime for machine learning, see [ONNX Runtime](#).

Common scenarios for machine learning solutions include:

- Predictive maintenance
- Inventory management
- Fraud detection
- Demand forecasting
- Intelligent recommendations
- Sales forecasting

## Checklist

- **Get started by first familiarizing yourself with Machine Learning**, and then choose which experience to begin with. You can follow along with steps to use a Jupyter notebook with Python, the visual drag-and-drop experience, or automated machine learning (AutoML).
  - [Machine Learning overview](#)
  - [Create your first machine learning experiment with a Jupyter notebook with Python](#)
  - [Visual drag-and-drop experiments](#)
  - [Use the AutoML UI](#)
  - [Configure your dev environment](#)
- **Experiment with more advanced tutorials** to predict taxi fees, classify images, and build a pipeline for batch scoring.
  - [Use AutoML to predict taxi fees](#)
  - [Classify images with scikit-learn](#)
  - [Build a Machine Learning pipeline for batch scoring](#)
- **Follow along with video tutorials** to learn more about the benefits of Machine Learning, such as no-code model building, MLOps, ONNX Runtime, model interpretability and transparency, and more.
  - [What's new with Machine Learning](#)
  - [Use AutoML to build models](#)
  - [Build zero-code models with Machine Learning designer](#)
  - [MLOps for managing the end-to-end lifecycle](#)

- Incorporating ONNX Runtime into your models
- Model interpretability and transparency
- Building models with R
- Review reference architectures for AI solutions

## Next steps

Explore other AI solution categories:

- [AI applications and agents](#)
- [Knowledge mining](#)

# AI applications and agents

11/9/2020 • 4 minutes to read • [Edit Online](#)

Infusing AI into an application can be difficult and time-consuming. Until recently, you needed both a deep understanding of machine learning and months of development to acquire data, train models, and deploy them at scale. Even then, success was not guaranteed. The path was filled with blockers, gotchas, and pitfalls causing teams to fail to realize value from their AI investments.

## AI applications

Microsoft Azure Cognitive Services remove these challenges and are designed to be productive, enterprise ready, and trusted. They make it possible for you to build on the latest breakthroughs in AI without building and deploying your own models; instead you can deploy AI models using just a few simple lines of code so that even without a large data science team, you can quickly create applications that see, hear, speak, understand, and even begin to reason.

Common scenarios for AI applications include:

- Sentiment analysis
- Object detection
- Translation
- Personalization
- Robotic process automation

As you get started, the checklist and resources below will help you plan your application development and deployment.

- Are you familiar with the multitude of capabilities and services offered within Azure Cognitive Services, and which ones in particular you will be using?
- Determine whether or not you have custom data with which you want to train and customize these models. There are Cognitive Services that are customizable.
- There are several ways to use Azure Cognitive Services. Explore the quickstart tutorials for getting up and running for both SDK and REST APIs. Note: the Cognitive Services SDKs are available for many popular dev languages, including C#, Python, Java, JavaScript and Go.
- Determine if you will need to deploy these Cognitive Services in containers.

## AI applications checklist

To get started, first familiarize yourself with the various categories and services within Azure Cognitive Services. Visit the product pages to learn more and to interact with demos to learn more about the capabilities available, such as vision, speech, language, and decision. There is also an e-book that walks through common scenarios and how to build your first application with Cognitive Services.

- [Cognitive Services](#)
- [Interactive demos across the product/service pages](#)
- [Building intelligent applications with cognitive APIs](#) (e-book)

Select the service you want to use across vision, language, speech, decision, or web search. Each category on the page offers a set of quick starts, tutorials, how-to guides, whether you want to use the REST API or SDKs.

You can also download the Intelligent Kiosk to experience and demo these services.

- [Cognitive Services documentation](#)
- [Building intelligent applications with cognitive APIs](#) (e-book)
- [Install the Intelligent Kiosk to familiarize yourself with Cognitive Services capabilities](#)

Learn more about container support for Azure Cognitive Services.

- [Container support in Azure Cognitive Services](#)

Review reference architectures for AI solutions.

- [AI + Machine Learning](#)

## AI agents

Microsoft's Azure AI platform aims to empower developers to innovate and accelerate their projects. Specifically for conversational AI, Azure offers the Azure Bot Service and Bot Framework SDK and tools enabling developers to build rich conversational experiences. Additionally, developers can use Azure Cognitive Services (domain-specific AI services available as APIs) like Language Understanding (LUIS), QnA Maker, and Speech service to add the abilities for your chatbot to understand and speak with your end users.

Common scenarios for conversational AI or chatbot solutions include:

- Informational Q&A chatbot
- Customer service or support chatbot
- IT help desk or HR chatbot
- e-commerce or sales chatbot
- Speech-enabled devices

### NOTE

We offer Power Virtual Agents, built on top of the Bot Framework, for developers who want to build a chatbot with a primarily no-code/low-code experience. Additionally, developers neither host the bot themselves, control the natural language or other AI models themselves with Cognitive Services.

## AI agents checklist

Familiarize yourself with Azure Bot Service and Microsoft Bot Framework.

- Bot Framework is an open-source offering that provides an SDK (available in C#, JavaScript, Python, and Java) to help you design, build, and test your bot. It also offers a free visual authoring canvas in Bot Framework Composer and a testing tool in Bot Framework Emulator.
- Azure Bot Service is a dedicated service within Azure that allows you to host or publish your bot in Azure and connect to popular channels.
- Read the [Azure Bot Service and Bot Framework overview](#)
- Learn about [Principles of bot design](#)
- Get the [latest versions of Bot Framework SDK and tools](#)

One of the simplest ways to get started is to use QnA Maker, part of Azure Cognitive Services, which can intelligently convert an FAQ document or website into a Q&A experience in minutes.

- [Create a bot with Q&A abilities quickly with QnA Maker](#)
- Test out the [QnA Maker service](#)

Download and use Bot Framework SDK and tools for bot development.

- [5 minute quickstart with Bot Framework Composer](#)
- [Build and test bots with Bot Framework SDK \(C#, JavaScript, Python\)](#)

Learn how to add Cognitive Services to make your bot even more intelligent.

- [A developer's guide to building AI applications](#) (e-book)
- Learn more about [Cognitive Services](#)

Learn how to build your own Virtual Assistant with Bot Framework solution accelerators, and select a common set of skills such as calendar, e-mail, point of interest, and to-do.

- [Bot Framework Virtual Assistant solution](#)

## Next steps

Explore other AI solution categories:

- [Machine learning](#)
- [Knowledge mining](#)

# Knowledge mining

11/9/2020 • 2 minutes to read • [Edit Online](#)

Knowledge mining refers to an emerging category of AI designed to simplify the process of accessing the latent insights contained within structured and unstructured data. It defines the process of using an AI pipeline to discover hidden patterns and actionable information from sets of structured and unstructured data in a scalable way.

Azure Cognitive Search is a managed cloud solution that gives developers APIs and tools for adding a rich search experience over private, heterogeneous content in web, mobile, and enterprise applications. It offers capabilities such as scoring, faceting, suggestions, synonyms, and geo-search to provide a rich user experience. Azure Cognitive Search is also the only cloud search service with built-in knowledge mining capabilities. Azure Cognitive Search acts as the orchestrator for your knowledge mining enrichment pipeline by following the steps to ingest, enrich, and explore and analyze.

Key scenarios for knowledge mining include:

- **Digital content management:** Help customers consume content more quickly by providing them relevant search results in your content catalog.
- **Customer support and feedback analysis:** Quickly find the right answer in documents and discover trends of what customers are asking for to improve customer experiences.
- **Data extraction and process management:** Accelerate processing documents by extracting key information and populating it in other business documentation.
- **Technical content review and research:** Quickly review documents and extract key information to make informed decisions.
- **Auditing and compliance management:** Quickly identify key areas and flag important ideas or information in documents.

## Checklist

- **Get started:** Access free knowledge mining solution accelerators, boot camps, and workshops.
  - [Knowledge mining solution accelerator](#)
  - [Knowledge mining workshop](#)
  - [Knowledge mining boot camp](#)
  - [Knowledge mining e-book](#)
- **Use power skills:** [Azure search power skills](#) provide useful functions deployable as custom skills for Azure Cognitive Search. The skills can be used as [templates](#) or starting points for your own custom skills. They also can be deployed and used as is if they happen to meet your requirements. We also invite you to contribute your own work by submitting a [pull request](#).
- **Explore additional resources:**
  - [Azure Cognitive Search overview](#)
  - [Built-in cognitive skills for text and image processing during indexing](#)
  - [Documentation resources for AI enrichment in Azure Cognitive Search](#)
  - [Design tips and tricks for AI enrichment](#)
  - [Full text search](#)

## Next steps

Explore other AI solution categories:

- [AI applications and agents](#)
- [Machine learning](#)

# Develop digital inventions in Azure

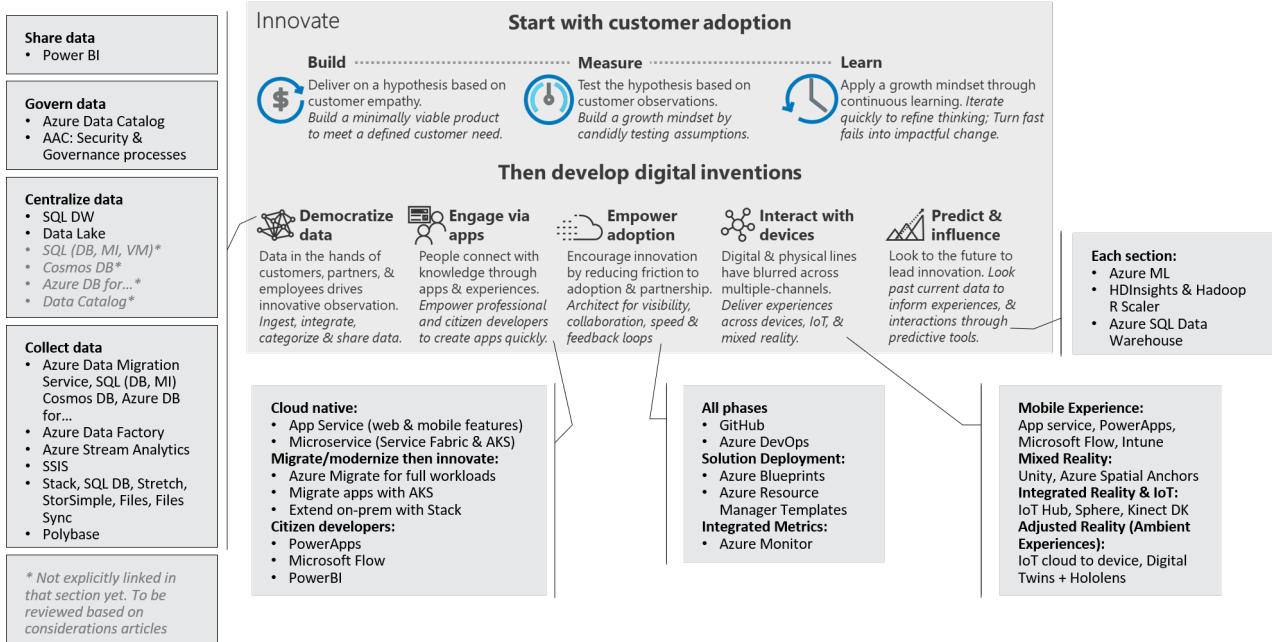
11/9/2020 • 2 minutes to read • [Edit Online](#)

Azure can help accelerate the development of each area of digital invention. This section of the Cloud Adoption Framework builds on the [Innovate methodology](#). This section shows how you can combine Azure services to create a toolchain for digital invention.

## Alignment to the methodology

There are many combinations of cloud-based tools for digital invention and innovation within Azure. The following article series demonstrates a few of the tools that closely align with the Innovate methodology. The following image shows an overview of how different tools align to each type of innovation.

### Innovation Toolchain in Azure



## Toolchain

Start with the overview page that relates to the type of digital invention you require to test your hypothesis. You start with that page for guidance you can act on and so that you can [build with customer empathy](#).

Here are the types of digital invention in this article series:

- Democratize data:** Tools for sharing data to solve information-related customer needs.
- Engage via applications:** Tools to create applications that engage customers beyond raw data.
- Empower adoption:** Tools to accelerate customer adoption through digital support for your build-measure-learn cycles.
- Interact with devices:** Tools to create different levels of ambient experiences for your customers.
- Predict and influence:** Tools for predictive analysis and integration of their output into applications.

# Tools to democratize data in Azure

11/9/2020 • 2 minutes to read • [Edit Online](#)

As described in the conceptual article on [democratizing data](#), you can deliver many innovations with little technical investment. Many major innovations require little more than raw data. Democratizing data is about investing as little resource as needed to engage your customers who use data to take advantage of their existing knowledge.

Starting with data is a quick way to test a hypothesis before expanding into broader, more costly digital inventions. As you refine more of the hypothesis and begin to adopt the inventions at scale, the following processes will help you prepare for operational support of the innovation.



## Alignment to the methodology

This type of digital invention can be accelerated through each phase of the following processes, as shown in the preceding image. Technical guidance to accelerate digital invention is listed in the table of contents on the left side of this page. Those articles are grouped by phase to align guidance with the overall methodology.

- **Share data:** The first step of democratizing data is to share openly.
- **Govern data:** Ensure that any sensitive data is secured, tracked, and governed before sharing.
- **Centralize data:** Sometimes you need to provide a centralized platform for data sharing and governance.
- **Collect data:** Migration, integration, ingestion, and virtualization can each collect existing data to be centralized, governed, and shared.

In every iteration, cloud adoption teams should go only as deep into the stack as they require to put the focus on customer needs over architecture. Delaying technical spikes in favor of customer needs accelerates validation of your hypothesis.

All guidance maps to the four preceding processes. Guidance ranges from the highest customer effect to the highest technical effect. Across each process, you'll see guidance on different potential ways that Azure can accelerate your ability to [build with customer empathy](#).

## Toolchain

In Azure, the following tools are commonly used to accelerate digital invention across the preceding phases:

- [Power BI](#)
- [Azure Data Catalog](#)
- [Azure Synapse Analytics](#)
- [Azure Cosmos DB](#)
- [Azure Database for PostgreSQL](#)
- [Azure Database for MySQL](#)

- [Azure Database for MariaDB](#)
- [Azure Database for PostgreSQL hyperscale](#)
- [Azure Data Lake Storage](#)
- [Azure Database Migration Service](#)
- [Azure SQL Database, with or without Azure SQL Managed Instance](#)
- [Azure Data Factory](#)
- [Azure Stream Analytics](#)
- [SQL Server Integration Services](#)
- [Azure Stack](#)
- [SQL Server Stretch Database](#)
- [Azure StorSimple](#)
- [Azure Files](#)
- [Azure file sync](#)
- [PolyBase](#)

As the invention approaches adoption at scale, the aspects of each solution require refinement and technical maturity. As that happens, more of these services are likely to be required. Use the table of contents on the left side of this page for Azure tools guidance relevant to your hypothesis-testing process.

## Get started

The table of contents on the left side of this page outlines many articles. These articles help you get started with each of the tools in this toolchain.

**NOTE**

Some links might leave the Cloud Adoption Framework to help you go beyond the scope of this framework.

# What is data classification?

11/9/2020 • 2 minutes to read • [Edit Online](#)

Data classification allows you to determine and assign value to your organization's data and provides a common starting point for governance. The data classification process categorizes data by sensitivity and business impact in order to identify risks. When data is classified, you can manage it in ways that protect sensitive or important data from theft or loss.

## Understand data risks, then manage them

Before any risk can be managed, it must be understood. In the case of data breach liability, that understanding starts with data classification. Data classification is the process of associating a metadata characteristic to every asset in a digital estate, which identifies the type of data associated with that asset.

Any asset identified as a potential candidate for migration or deployment to the cloud should have documented metadata to record the data classification, business criticality, and billing responsibility. These three points of classification can go a long way to understanding and mitigating risks.

## Classifications Microsoft uses

The following is a list of classifications Microsoft uses. Depending on your industry or existing security requirements, data classification standards might already exist within your organization. If no standard exists, you might want to use this sample classification to better understand your own digital estate and risk profile.

- **Non-business:** Data from your personal life that doesn't belong to Microsoft.
- **Public:** Business data that is freely available and approved for public consumption.
- **General:** Business data that isn't meant for a public audience.
- **Confidential:** Business data that can cause harm to Microsoft if overshared.
- **Highly confidential:** Business data that would cause extensive harm to Microsoft if overshared.

## Tagging data classification in Azure

Resource tags are a good approach for metadata storage, and you can use these tags to apply data classification information to deployed resources. Although tagging cloud assets by classification isn't a replacement for a formal data classification process, it provides a valuable tool for managing resources and applying policy. [Azure Information Protection](#) is an excellent solution to help you classify data itself, regardless of where it resides (on-premises, in Azure, or somewhere else). Consider it as part of an overall classification strategy.

## Take action

Take action by defining and tagging assets with a defined data classification.

- [Choose one of the actionable governance guides](#) for examples of applying tags across your portfolio.
- Review the [naming and tagging standards](#) article to define a more comprehensive tagging standard.
- For additional information on resource tagging in Azure, see [Use tags to organize your Azure resources and management hierarchy](#).

## Next steps

Continue learning from this article series by reviewing the article on securing sensitive data. The next article

contains applicable insights if you are working with data that is classified as confidential or highly confidential.

[Secure sensitive data](#)

# Collect data through the migration and modernization of existing data sources

11/9/2020 • 2 minutes to read • [Edit Online](#)

Companies often have different kinds of existing data that they can [democratize](#). When a customer hypothesis requires the use of existing data to build modern solutions, a first step might be the migration and modernization of data to prepare for inventions and innovations. To align with existing migration efforts within a cloud adoption plan, you can more easily do the migration and modernization within the [Migrate methodology](#).

## Use of this article

This article outlines a series of approaches that align with the Migrate methodology. You can best align these approaches to the standard migration toolchain.

During the Assess phase within the Migrate methodology, a cloud adoption team assesses the current state and desired future state for the migrated asset. When that process is part of an innovation effort, both cloud adoption teams can use this article to help make those assessments.

## Primary toolset

When you migrate and modernize on-premises data, the most common Azure tool choice is [Azure Database Migration Service](#). This service is part of the broader [Azure Migrate](#) toolchain. For existing SQL Server data sources, [Data Migration Assistant](#) can help you assess and migrate a small number of data structures.

To support Oracle and NoSQL migrations, you can also use [Database Migration Service](#) for certain types of source-to-target databases. Examples include migrating Oracle databases to PostgreSQL or MongoDB databases to Azure Cosmos DB. More commonly, adoption teams use partner tools or custom scripts to migrate to Azure Cosmos DB, Azure HDInsight, or virtual machine options based on infrastructure as a service (IaaS).

## Considerations and guidance

When you use Azure Database Migration Service to migrate and modernize data, it's important to understand:

- The current platform for hosting the data source.
- The current version.
- The future platform and version that best supports the customer hypothesis or target.

The following table shows source and target pairs to review with the migration team. Each pair includes a tool choice and a link to a related guide.

### Migration type

With an offline migration, application downtime starts when the migration starts. With an online migration, downtime is limited to the time to cut over at the end of migration.

We suggest that you decide your acceptable business downtime and test an offline migration. You do so to check if the restoration time meets the acceptable downtime. If the restoration time is unacceptable, do an online migration.

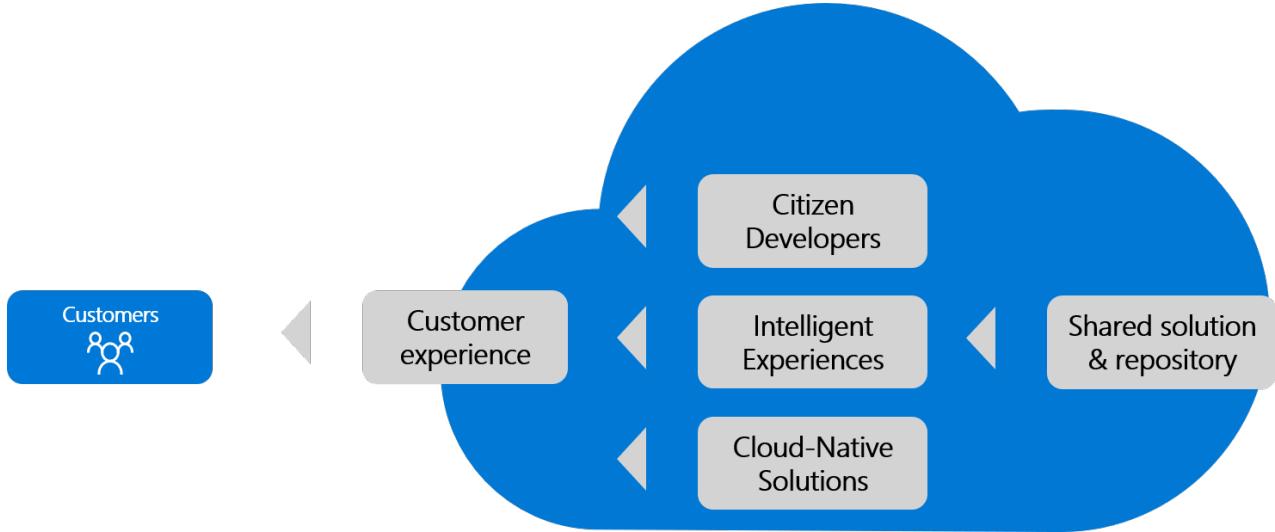
SOURCE	TARGET	TOOL	MIGRATION TYPE	GUIDANCE
--------	--------	------	----------------	----------

SOURCE	TARGET	TOOL	MIGRATION TYPE	GUIDANCE
SQL Server	Azure SQL Database	Database Migration Service	Offline	<a href="#">Tutorial</a>
SQL Server	Azure SQL Database	Database Migration Service	Online	<a href="#">Tutorial</a>
SQL Server	Azure SQL Managed Instance	Database Migration Service	Offline	<a href="#">Tutorial</a>
SQL Server	Azure SQL Managed Instance	Database Migration Service	Online	<a href="#">Tutorial</a>
RDS SQL Server	Azure SQL Database or Azure SQL Managed Instance	Database Migration Service	Online	<a href="#">Tutorial</a>
MySQL	Azure Database for MySQL	Database Migration Service	Online	<a href="#">Tutorial</a>
PostgreSQL	Azure Database for PostgreSQL	Database Migration Service	Online	<a href="#">Tutorial</a>
MongoDB	Azure Cosmos DB's API for MongoDB	Database Migration Service	Offline	<a href="#">Tutorial</a>
MongoDB	Azure Cosmos DB's API for MongoDB	Database Migration Service	Online	<a href="#">Tutorial</a>

# Tools to engage via applications in Azure

11/9/2020 • 2 minutes to read • [Edit Online](#)

As described in [Engage via applications](#), applications can be an important aspect of an MVP solution. Applications are often required for testing a hypothesis. This article helps you learn the tools Azure provides to accelerate development of those applications.



## Alignment to the methodology

You can accelerate this type of digital invention through each of the following listed approaches. The preceding image also shows these approaches. Technical guidance for accelerating digital invention is listed in the table of contents on the left side of this page. Those articles are grouped by their approaches to aligning guidance with the overall methodology.

For this article, assume all inventions that result in an application stem from a shared solution as described in [Empower adoption](#). Also assume each application results in some type of customer experience for both internal and external customers.

Based on these assumptions, the following three paths are the most common for cloud adoption teams who are developing digital inventions:

- **Citizen developers**: Before engaging professional developers, business subject matter experts use citizen developer tools. These tools rapidly test and validate that a customer hypothesis can meet the needs of that customer.
- **Intelligent experiences**: Create modern experiences by using cloud platforms to drive rapid deployment and short feedback loops. Expand on web applications to infuse intelligence or even integrate bots.
- **Cloud-native**: Build a new invention that naturally takes advantage of cloud capabilities.

Each path results in advantages and disadvantages that are both short-term and long-term. When the cloud governance team, the cloud operations team, and the cloud center of excellence team are ready to support every approach, you can accelerate adoption with minimal effect on sustainable business operations.

## Toolchain

Depending on the path that the cloud adoption team takes, Azure provides tools to accelerate the team's ability to build with customer empathy. The following list of Azure offerings is grouped based on the preceding decision

paths. These offerings include:

- Azure App Service
- Azure Kubernetes Service (AKS)
- Azure Migrate
- Azure Stack
- Power Apps
- Power Automate
- Power BI

## Get started

The table of contents on the left side of this page outlines many articles. These articles help you get started with each of the tools in this toolchain.

**NOTE**

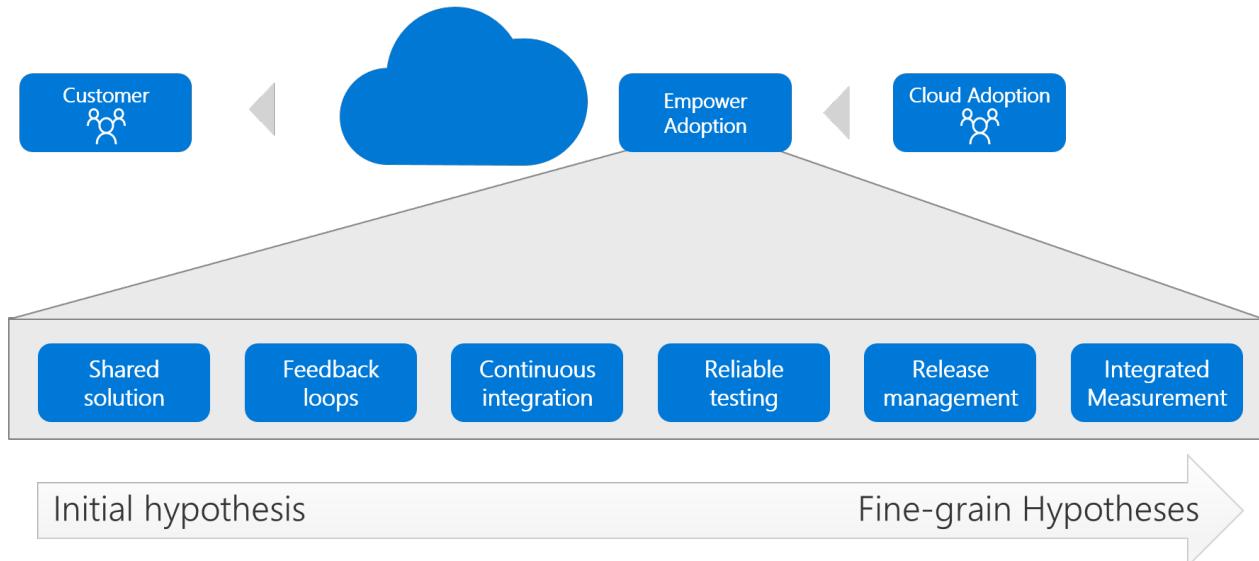
Some links might leave the Cloud Adoption Framework to help you go beyond the scope of this framework.

# Tools to empower adoption in Azure

11/9/2020 • 2 minutes to read • [Edit Online](#)

As described in [Empower adoption](#), building true innovation at scale requires an investment in removing friction that could slow adoption. In the early stages of testing a hypothesis, a solution is small. The investment in removing friction is likely small as well. As hypotheses prove true, the solution and the investment in empowering adoption grows. This article provides key links to help you get started with each stage of maturity.

Empower adoption incrementally, as hypotheses mature



## Alignment to the methodology

You can accelerate this type of digital invention through the following levels of maturity. These levels align with the maturity model in the preceding image. Technical guidance to accelerate digital invention is listed in the table of contents on the left side of this page. Those articles are grouped by maturity level.

- **Shared solution:** Establish a centralized repository for all aspects of the solution.
- **Feedback loops:** Ensure feedback loops can be managed consistently throughout iterations.
- **Continuous integration:** Regularly build and consolidate a solution.
- **Reliable testing:** Validate solution quality and expected changes to drive ensuring measurements.
- **Solution deployment:** Deploy a solution to allow a team to quickly share changes with customers.
- **Integrated measurement:** Add learning metrics to the feedback loop for clear analysis by the full team.

## Toolchain

For adoption teams that are mature professional development teams with many contributors, the Azure toolchain starts with GitHub and Azure DevOps.

As your need grows, you can expand this foundation to use other tool features. The expanded foundation might involve tools like:

- Azure Blueprints
- Azure Policy
- Azure Resource Manager templates

- Azure Monitor

The table of contents on the left side of this page lists guidance for each tool and aligns with the previously described maturity model.

## Get started

The table of contents on the left side of this page outlines many articles. These articles help you get started with each of the tools in this toolchain.

**NOTE**

Some links might leave the Cloud Adoption Framework to help you go beyond the scope of this framework.

# Machine Learning Operations with Azure Machine Learning

11/9/2020 • 2 minutes to read • [Edit Online](#)

Machine Learning Operations (MLOps) is based on DevOps principles and practices that increase workflow efficiencies like continuous integration, delivery, and deployment. MLOps applies these principles to the machine learning process in order to:

- Experiment and develop models more quickly.
- Deploy models to production more quickly.
- Practice and refine quality assurance.

Azure Machine Learning provides the following MLOps capabilities:

- **Create reproducible pipelines.** Machine Learning pipelines enable you to define repeatable and reusable steps for your data preparation, training, and scoring processes.
- **Create reusable software environments** for training and deploying models.
- **Register, package, and deploy models from anywhere.** You can track the associated metadata required to use the model.
- **Capture the governance data for the end-to-end lifecycle.** The logged information can include who is publishing models, why changes were made, and when models were deployed or used in production.
- **Notify and alert on events in the lifecycle.** For example, you can get alerts for experiment completion, model registration, model deployment, and data drift detection.
- **Monitor applications for operational and machine learning-related issues.** Compare model inputs between training and inference, explore model-specific metrics, and provide monitoring and alerts on your machine learning infrastructure.
- **Automate the end-to-end machine learning lifecycle with Azure Machine Learning and Azure Pipelines.** With pipelines, you can frequently update models, test new models, and continuously roll out new machine learning models alongside your other applications and services.

## Best practices for MLOps with Azure Machine Learning

Models differ from code because they have an organic shelf life and will deteriorate unless maintained. After they're deployed, they can add real business value, and this gets easier when data scientists are given the tools to adopt standard engineering practices.

MLOps with Azure helps you:

- Create reproducible models and reusable training pipelines.
- Simplify model packaging, validation, and deployment for quality control and A/B testing.
- Explain and observe model behavior, and automate the retraining process.

MLOps improves the quality and consistency of your machine learning solutions. To learn more about how to use Azure Machine Learning to manage the lifecycle of your models, see [MLOps: Model management, deployment, and monitoring with Azure Machine Learning](#).

## Next steps

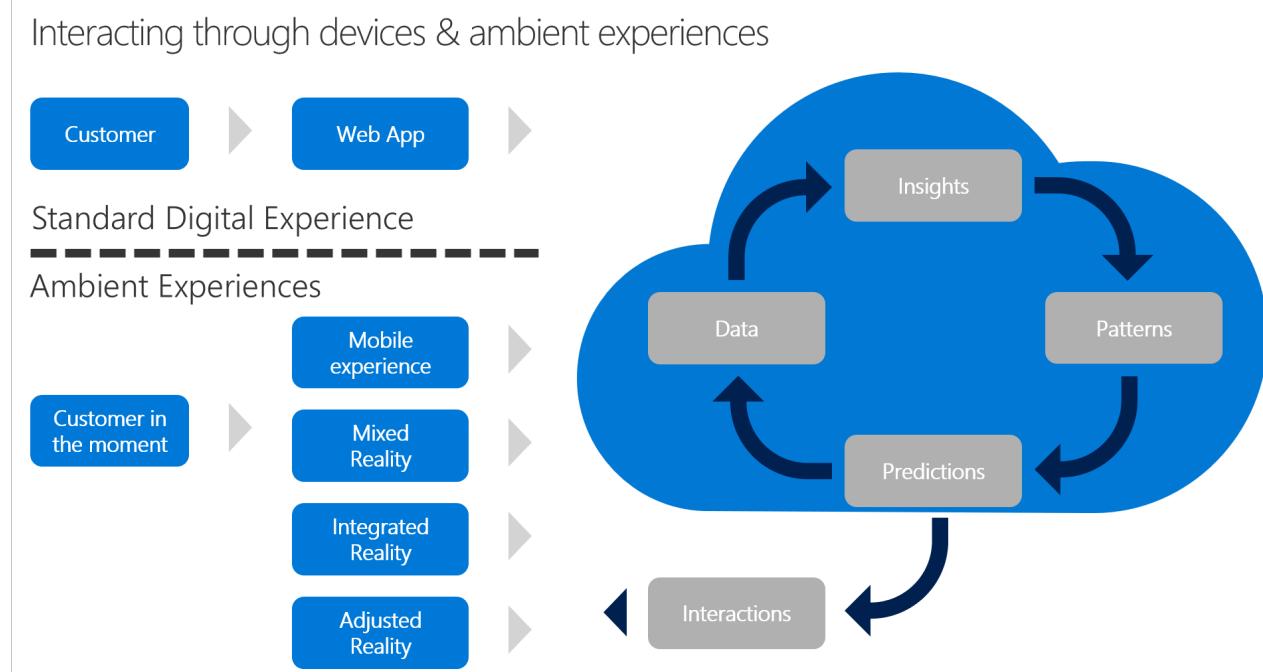
Learn more by reading and exploring the following resources:

- [MLOps: Model management, deployment, and monitoring with Azure Machine Learning](#)
- How and where to [deploy models with Azure Machine Learning](#)
- Tutorial: [Deploy an image classification model in ACI](#)
- [End-to-end MLOps examples repo](#)
- [CI/CD of machine learning models with Azure Pipelines](#)
- Create clients that [consume a deployed model](#)
- [Machine learning at scale](#)
- [Azure AI reference architectures and best practices repo](#)

# Tools to interact with devices in Azure

11/9/2020 • 2 minutes to read • [Edit Online](#)

As described in the conceptual article on [interacting with devices](#), the devices used to interact with a customer depend on the amount of ambient experience required to deliver the customer's need and empower adoption. Speed from the trigger that prompts the customer's need and your solution's ability to meet that need are determining factors in repeat usage. Ambient experiences help accelerate that response time and create a better experience for your customers by embedding your solution in the customers' immediate surroundings.



## Alignment to the methodology

This type of digital invention can be delivered through any of the following levels of ambient experience. These levels align with the methodology as shown in the preceding image. The table of contents on the left side of this page lists technical guidance to accelerate digital invention. Those articles are grouped by level of ambient experience to align with the methodology.

- **Mobile experience:** Mobile apps are commonly part of a customer's surroundings. In some scenarios, a mobile device might provide enough interactivity to make a solution ambient.
- **Mixed reality:** Sometimes a customer's natural surroundings must be altered through mixed reality. Engaging a customer within that mixed reality can provide a form of ambient experience.
- **Integrated reality:** Moving closer to true ambience, integrated reality solutions focus on the use of a customer's physical device to integrate the solution into natural behaviors.
- **Adjusted reality:** When any of the preceding solutions use predictive analysis to provide an interaction with a customer within that customer's natural surroundings, that solution creates the highest form of ambient experience.

## Toolchain

In Azure, you commonly use the following tools to accelerate digital invention across each of the preceding levels of ambient solutions. These tools are grouped based on the amount of experience required to reduce complexity in aligning tools with those experiences.

CATEGORY	TOOLS
Mobile experiences	<ul style="list-style-type: none"> <li>• Azure App Service</li> <li>• Power Apps</li> <li>• Power Automate</li> <li>• Intune</li> </ul>
Mixed reality	<ul style="list-style-type: none"> <li>• Unity</li> <li>• Azure Spatial Anchors</li> <li>• HoloLens</li> </ul>
Integrated reality	<ul style="list-style-type: none"> <li>• Azure IoT Hub</li> <li>• Azure Sphere</li> <li>• Azure Kinect DK</li> </ul>
Adjusted reality	<ul style="list-style-type: none"> <li>• IoT cloud to device</li> <li>• Azure Digital Twins + HoloLens</li> </ul>

## Get started

The table of contents on the left side of this page outlines many articles. These articles help you get started with each of the tools in this toolchain.

### NOTE

Some links might leave the Cloud Adoption Framework to help you go beyond the scope of this framework.

# Use innovation tools to predict and influence

11/9/2020 • 2 minutes to read • [Edit Online](#)

Using AI, your company can make predictions about customers' needs and automate business processes. You also can discover information lying latent in unstructured data and deliver new ways to engage with customers to deliver better experiences.

You can accelerate this type of digital invention through each of the following solution areas. Best practices and technical guidance to accelerate digital invention are listed in the table of contents on the left side of this page. Those articles are grouped by solution area:

- Machine learning
- AI applications and agents
- Knowledge mining

## Get started

The table of contents on the left side of this page outlines many articles. These articles help you get started with each of the solution areas.

### NOTE

Some links might leave the Cloud Adoption Framework to help you go beyond the scope of this framework.

# What is machine learning?

11/9/2020 • 6 minutes to read • [Edit Online](#)

Machine learning is a data science technique that allows computers to use existing data to forecast future behaviors, outcomes, and trends. By using machine learning, computers learn without being explicitly programmed.

Forecasts or predictions from machine learning can make applications and devices smarter. For example, when you shop online, machine learning helps recommend other products you might want based on what you've bought. Or when your credit card is swiped, machine learning compares the transaction to a database of transactions and helps detect fraud. And when your robot vacuum cleaner vacuums a room, machine learning helps it decide whether the job is done.

## Machine learning tools to fit each task

Azure Machine Learning provides all the tools developers and data scientists need for their machine learning workflows, including:

- The [Azure Machine Learning designer \(preview\)](#): Drag-n-drop modules to build your experiments and then deploy pipelines
- Jupyter notebooks: use our [example notebooks](#) or create your own notebooks to use our SDK for Python samples.
- R scripts or notebooks in which you use the [SDK for R](#) to write your own code, or use the R modules in the designer.
- The [many models solution accelerator \(preview\)](#) builds on Azure Machine Learning and enables you to train, operate, and manage hundreds or even thousands of machine learning models.
- [Visual Studio Code extension](#).
- [Machine learning CLI](#).
- Open-source frameworks such as PyTorch, TensorFlow, and scikit-learn and many more
- [Reinforcement learning](#) with Ray RLlib.

You can even use [MLflow to track metrics and deploy models](#) or [kubeflow](#) to build end-to-end workflow pipelines.

## Build machine learning models in Python or R

Start training on your local machine using the Azure Machine Learning [Python SDK](#) or [R SDK](#). Then, you can scale out to the cloud. With many available [compute targets](#), like Azure Machine Learning compute and [Azure Databricks](#), and with [advanced hyperparameter tuning services](#), you can build better models faster by using the power of the cloud. You can also [automate model training and tuning](#) using the SDK.

## Build machine learning models with no-code tools

For code-free or low-code training and deployment, try:

- Azure Machine Learning designer (preview)

Use the designer to prep data, train, test, deploy, manage, and track machine learning models without writing any code. There is no programming required, you visually connect datasets and modules to construct your model. Try out the [designer tutorial](#).

Learn more in the [Azure Machine Learning designer overview article](#).

- Automated machine learning (AutoML) UI

Learn how to create [AutoML experiments](#) in the easy-to-use interface.

## MLOps: Deploy and lifecycle management

Machine Learning operations (MLOps) is based on [DevOps](#) principles and practices that increase the efficiency of workflows. For example, continuous integration, delivery, and deployment. MLOps applies these principles to the machine learning process, with the goal of:

- Faster experimentation and development of models
- Faster deployment of models into production
- Quality assurance

When you have the right model, you can easily use it in a web service, on an IoT device, or from Power BI. For more information, see [Deploy models with Azure Machine Learning](#).

Then you can manage your deployed models by using the [Azure Machine Learning SDK for Python](#), [Azure Machine Learning studio](#), or the [Machine learning CLI](#).

These models can be consumed and return predictions in [Real time](#) or [asynchronously](#) on large quantities of data.

And with advanced [machine learning pipelines](#), you can collaborate on each step from data preparation, model training and evaluation, through deployment. Pipelines allow you to:

- Automate the end-to-end machine learning process in the cloud
- Reuse components and only rerun steps when needed
- Use different compute resources in each step
- Run batch scoring tasks

If you want to use scripts to automate your machine learning workflow, the [Machine learning CLI](#) provides command-line tools that perform common tasks, such as submitting a training run or deploying a model.

To get started using Azure Machine Learning, see [Next steps](#).

## Automated Machine Learning

Data scientists spend an inordinate amount of time iterating over models during the experimentation phase. The whole process of trying out different algorithms and hyperparameter combinations until an acceptable model is built is extremely taxing for data scientists, due to the monotonous and non-challenging nature of work. While this is an exercise that yields massive gains in terms of the model efficacy, it sometimes costs too much in terms of time and resources and thus may have a negative return on investment (ROI).

This is where automated machine learning (AutoML) comes in. It uses the concepts from the research paper on probabilistic matrix factorization and implements an automated pipeline of trying out intelligently-selected algorithms and hypermeter settings, based on the heuristics of the data presented, keeping into consideration the given problem or scenario. The result of this pipeline is a set of models that are best suited for the given problem and dataset.

For more information on AutoML, see [AutoML and MLOps with Azure Machine Learning](#).

## Responsible ML

Throughout the development and use of AI systems, trust must be at the core. Trust in the platform, process, and models. As AI and autonomous systems integrate more into the fabric of society, it's important to proactively make an effort to anticipate and mitigate the unintended consequences of these technologies.

- Understand your models and build for fairness: explain model behavior and uncover features that have the most impact on predictions. Use built-in explainers for both glass-box and black-box models during model training and inference. Use interactive visualizations to compare models and perform what-if analysis to improve model accuracy. Test your models for fairness using state-of-the-art algorithms. Mitigate unfairness throughout the machine learning lifecycle, compare mitigated models, and make intentional fairness versus accuracy trade-offs as desired.
- Protect data privacy and confidentiality: build models that preserve privacy using the latest innovations in differential privacy, which injects precise levels of statistical noise in data to limit the disclosure of sensitive information. Identify data leaks and intelligently limit repeat queries to manage exposure risk. Use encryption and confidential machine learning (coming soon) techniques specifically designed for machine learning to securely build models using confidential data.
- Control and govern through every step of the machine learning process: access built-in capabilities to automatically track lineage and create an audit trail across the machine learning lifecycle. Obtain full visibility into the machine learning process by tracking datasets, models, experiments, code, and more. Use custom tags to implement model data sheets, document key model metadata, increase accountability, and ensure responsible process.

Learn more about how to implement [Responsible ML](#).

## Integration with other services

Azure Machine Learning works with other services on the Azure platform, and also integrates with open source tools such as Git and MLflow.

- Compute targets such as Azure Kubernetes Service, Azure Container Instances, Azure Databricks, Azure Data Lake Analytics, and Azure HDInsight. For more information on compute targets, see [What are compute targets?](#).
- Azure Event Grid. For more information, see [Consume Azure Machine Learning events](#).
- Azure Monitor. For more information, see [Monitoring Azure Machine Learning](#).
- Data stores such as Azure Storage accounts, Azure Data Lake Storage, Azure SQL Database, Azure Database for PostgreSQL, and Azure open datasets. For more information, see [Access data in Azure Storage services](#) and [create datasets with Azure open datasets](#).
- Azure Virtual Network. For more information, see [Secure experimentation and inference in a virtual network](#).
- Azure Pipelines. For more information, see [Train and deploy machine learning models](#).
- Git repository logs. For more information, see [Git integration](#).
- MLflow. For more information, see [MLflow to track metrics and deploy models](#).
- Kubeflow. For more information, see [Build end-to-end workflow pipelines](#).
- Secure communications. Your Azure Storage account, compute targets, and other resources can be used securely inside a virtual network to train models and perform inference. For more information, see [Secure experimentation and inference in a virtual network](#).

## Next steps

- Review machine learning white papers and e-books on [Machine Learning studio](#) and [Machine Learning service](#).
- Review [AI + Machine Learning architectures](#).

# What are AI applications?

11/9/2020 • 4 minutes to read • [Edit Online](#)

In Azure, you can build intelligent applications faster by using the tools and technologies of your choice and built-in AI.

- **Easily build and deploy anywhere:** Use your team's existing skill set and the tools you know to build intelligent applications and deploy them without a change in code. You can build once and then deploy in the cloud, on-premises, and to edge devices. You can be confident of global distribution to more datacenters than with any other provider.
- **Create an impact by using an open platform:** Choose your favorite technologies, which can be open source. Azure supports a range of deployment options, popular stacks and languages, and a comprehensive set of data engines. Capitalize on this flexibility, plus the performance, scale, and security delivered by Microsoft technologies to build applications for any scenario.
- **Develop applications with built-in intelligence:** Building intelligent applications using Azure is easy, because no other platform brings analytics and native AI to your data wherever it lives and in the languages you use. You can take advantage of a rich set of [cognitive APIs](#) to easily build new experiences into your applications for human-like intelligence.

## What is Azure Cognitive Services?

Azure Cognitive Services can simplify how you integrate AI capabilities and breakthroughs into your applications with a few simple lines of code. It supports you to create applications that see, hear, speak, understand, and even start to reason between your business processes. Cognitive Services provides AI intelligence in a form that's easy to use and incorporate into your applications.

Cognitive Services is made up of APIs, SDKs, and services available to help developers build intelligent applications without having direct AI or data science skills or knowledge. Cognitive Services enables developers to easily add cognitive features into their applications. The catalog of services within Cognitive Services can be categorized into five main parts: vision, speech, language, web search, and decision.

### Vision APIs

SERVICE NAME	SERVICE DESCRIPTION
Computer Vision	Computer Vision provides you with access to advanced algorithms for processing images and returning information.
Custom Vision	Custom Vision allows you to build custom image classifiers.
Face	The Face service provides access to advanced face algorithms that detect and recognize facial attributes.
Form Recognizer (preview)	Form Recognizer identifies and extracts key-value pairs and table data from form documents. It then outputs structured data, which includes the relationships, in the original file.
Ink Recognizer (preview)	Ink Recognizer allows you to recognize and analyze digital ink-stroke data, shapes, and handwritten content, and output a document structure with all recognized entities.

Service Name	Service Description
<a href="#">Video Indexer</a>	Video Indexer enables you to extract insights from your videos.

## Speech APIs

Service Name	Service Description
<a href="#">Speech</a>	Speech service adds speech-enabled features to applications.
<a href="#">Speaker Recognition (preview)</a>	The Speaker Recognition API provides algorithms for Speaker Identification and verification.
<a href="#">Bing Speech (retiring)</a>	The Bing Speech API provides you with an easy way to create speech-enabled features in your applications.
<a href="#">Translator speech (retiring)</a>	Translator speech is a machine translation service.

## Language APIs

Service Name	Service Description
<a href="#">Language Understanding (LUIS)</a>	The Language Understanding service (LUIS) allows your application to understand what a person wants in their own words.
<a href="#">QnA Maker</a>	QnA Maker allows you to build a question-and-answer service from your semistructured content.
<a href="#">Text Analytics</a>	Text Analytics provides natural language processing over raw text for sentiment analysis, key phrase extraction, and language detection.
<a href="#">Translator</a>	Translator provides machine-based text translation in near real time.

## Decision APIs

Service Name	Service Description
<a href="#">Anomaly Detector (preview)</a>	Anomaly Detector allows you to monitor and detect abnormalities in your time series data.
<a href="#">Content Moderator</a>	Content Moderator provides monitoring for possible offensive, undesirable, and risky content.
<a href="#">Personalizer</a>	Personalizer allows you to learn from users' real-time behavior in order to choose the most tailored experience for them.

## Supported cultural languages

Cognitive Services supports a wide range of cultural languages at the service level. You can find the language availability for each API in the [supported languages list](#).

## Secure resources

Cognitive Services provides a layered security model, which includes [authentication](#) via Azure Active Directory credentials, a valid resource key, and [Azure Virtual Network](#).

## Container support

Cognitive Services provides containers for deployment in the cloud or on-premises. Learn more about [Cognitive Services containers](#).

## Certifications and compliance

Cognitive Services has been awarded certifications such as CSA STAR certification, FedRAMP Moderate, and HIPAA BAA.

You can [download](#) certifications for your own audits and security reviews.

To understand privacy and data management, go to the [Microsoft Trust Center](#).

## How are Cognitive Services and Azure Machine Learning similar?

Cognitive Services and Azure Machine Learning have the common goal of applying AI to enhance business operations. How each one provides this capability in the respective offerings is different. Generally, the audiences are different:

- Cognitive Services is for developers without machine learning experience.
- Machine Learning is tailored for data scientists.

## How is a cognitive service different from machine learning?

A cognitive service provides a trained model for you. This model brings data and an algorithm together and is available from a REST API or SDK. You can implement this service within minutes depending on your scenario. A cognitive service provides answers to general problems such as key phrases in text or item identification in images.

Machine learning is a process that generally requires a longer period of time to implement successfully. This time is spent on data collection, cleaning, transformation, algorithm selection, model training, and deployment to get to the same level of functionality provided by a cognitive service. With machine learning, it's possible to provide answers to highly specialized or specific problems. Machine learning problems require familiarity with the specific subject matter and data of the problem under consideration and expertise.

## Next steps

- Learn more about [Cognitive Services](#).
- Find [best practices for AI architectures](#).

# What are AI agents?

11/9/2020 • 6 minutes to read • [Edit Online](#)

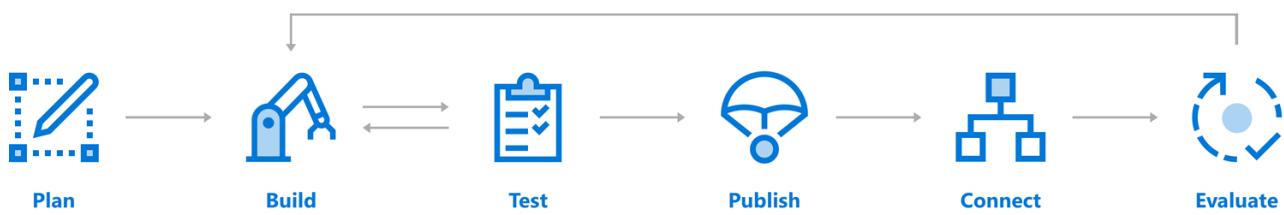
Users are engaging more and more with conversational interfaces, which can present a more natural experience where humans express their needs through natural language and quickly complete tasks. For many companies, conversational AI applications are becoming a competitive differentiator. Many organizations are strategically making bots available within the same messaging platforms in which their customers spend time.

Organizations around the world are transforming their businesses with conversational AI, which can promote more efficient and natural interactions with both their customers and their employees. Here are a few common use cases:

- Customer support
- Enterprise assistant
- Call center optimization
- In-car voice assistant

## Build a bot

Azure Bot Service and Bot Framework offer an integrated set of tools and services to help with this process. Choose your favorite development environment or command-line tools to create your bot. SDKs exist for C#, JavaScript, TypeScript, and Python. The SDK for Java is under development. We provide tools for various stages of bot development to help you design and build bots.



### Plan

Having a thorough understanding of the goals, processes, and user needs is important to the process of creating a successful bot. Before you write code, review the bot [design guidelines](#) for best practices, and identify the needs for your bot. You can create a simple bot or include more sophisticated capabilities such as speech, natural language understanding, and question answering.

While you design your bot in the Plan phase, consider these aspects:

- Define bot personas:
  - What should your bot look like?
  - What should it be named?
  - What's your bot's personality? Does it have a gender?
  - How should your bot handle difficult situations and questions?
- Design conversation flow:
  - What type of conversations can you expect for your use cases?
- Define an evaluation plan:
  - How would you measure success?
  - What measurements do you want to use to improve your service?

To learn more about how to design your bot, see [Principles of bot design](#).

## Build

Your bot is a web service that implements a conversational interface and communicates with the Bot Framework Service to send and receive messages and events. The Bot Framework Service is one of the components of Azure Bot Service and Bot Framework. You can create bots in any number of environments and languages. You can start your bot development in the [Azure portal](#) or use [C#, JavaScript, or Python](#) templates for local development. You also have access to a variety of [samples](#) that showcase many of the capabilities available through the SDK. These samples are great for developers who want a more feature-rich starting point.

As part of the Azure Bot Service and Bot Framework, we offer additional components you can use to extend the functionality of your bot.

FEATURE	DESCRIPTION	LINK
Add natural language processing	Enable your bot to understand natural language, understand spelling errors, use speech, and recognize the user's intent.	How to use <a href="#">LUIS</a>
Answer questions	Add a knowledge base to answer questions users ask in a more natural, conversational way.	How to use <a href="#">QnA Maker</a>
Manage multiple models	If you use more than one model, such as for LUIS and QnA Maker, intelligently determine when to use which one during your bot's conversation.	<a href="#">Dispatch tool</a>
Add cards and buttons	Enhance the user experience with media other than text, such as graphics, menus, and cards.	How to add <a href="#">cards</a>

### NOTE

This table isn't a comprehensive list. For more information, see the [Azure Bot Service documentation](#).

## Test

Bots are complex applications with many different parts that work together. Like any other complex application, this complexity can lead to some interesting bugs or cause your bot to behave differently than expected. Before you publish your bot, test it. We provide several ways to test bots before they're released for use:

- Test your bot locally with the [emulator](#). The Bot Framework Emulator is a stand-alone application that not only provides a chat interface but also debugging and interrogation tools to help you understand how and why your bot does what it does. The emulator can be run locally alongside your in-development bot application.
- Test your bot on the [web](#). After your bot is configured through the Azure portal, it can also be reached through a web chat interface. The web chat interface is a great way to grant access to your bot to testers and other people who don't have direct access to the running code.
- [Unit test your bot](#) with the July update of the Bot Framework SDK.

## Publish

When you're ready to make your bot available on the web, [publish it to Azure](#) or to your own web service or datacenter. Having an address on the public internet is the first step to bringing your bot to life on your site or inside chat channels.

## Connect

Connect your bot to channels such as Facebook, Messenger, Kik, Skype, Slack, Microsoft Teams, Telegram, text/SMS,

Twilio, Cortana, and Skype. Bot Framework does most of the work necessary to send and receive messages from all of these different platforms. Your bot application receives a unified, normalized stream of messages no matter number and type of channels to which it's connected. For information on how to add channels, see [Channels](#).

## Evaluate

Use the data collected in the Azure portal to identify opportunities to improve the capabilities and performance of your bot. You can get service-level and instrumentation data like traffic, latency, and integrations. Analytics also provide conversation-level reporting on user, message, and channel data. For more information, see [How to gather analytics](#).

## Patterns for common use cases

There are common patterns used for implementation of a conversational AI application:

- **Knowledge base:** A knowledge bot can be designed to provide information about virtually any subject. For example, one knowledge bot might answer questions about events such as "what bot events are there at this conference?" Or "when is the next reggae show?" Another bot might answer IT-related questions such as "how do I update my operating system?" Yet another bot might answer questions about contacts such as "who is john doe?" Or "what is jane doe's email address?"

For information on the design elements for knowledge bots, see [Design knowledge bots](#).

- **Hand off to a human:** No matter how much AI a bot possesses, there might still be times when it needs to hand off the conversation to a human being. In such cases, the bot should recognize when it needs to hand off and provide the user with a smooth transition.

For information on the patterns to hand off, see [Transition conversations from bot to human](#).

- **Embed a bot in an application:** Although bots most commonly exist outside of applications, they can also be integrated with applications. For example, you could embed a [knowledge bot](#) within an application to help users find information. You could also embed a bot within a help desk application to act as the first responder to incoming user requests. The bot could independently resolve simple issues and [hand off](#) more complex issues to a human agent.

For information on the ways to integrate your bot within an application, see [Embed a bot in an application](#).

- **Embed a bot in a website:** Like embedding bots in applications, bots can also be embedded within a website to enable multiple modes of communication across channels.

For information on the ways to integrate your bot within a website, see [Embed a bot in a website](#).

## Next steps

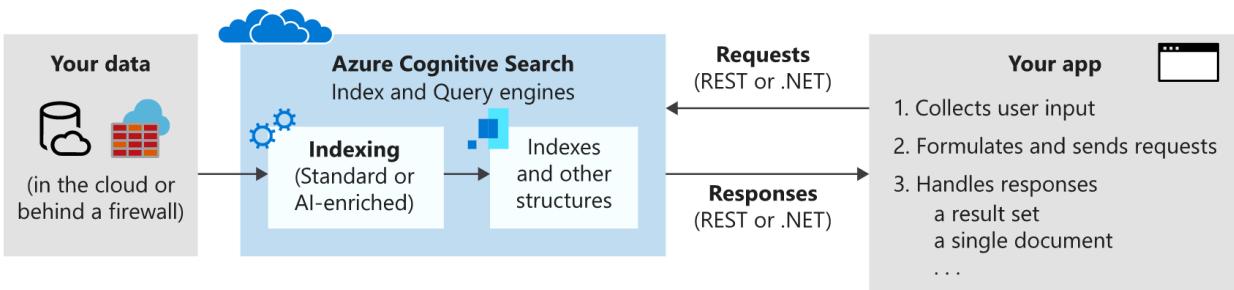
- Review machine learning white papers and e-books about [Azure Bot Service](#).
- Review [AI + Machine Learning architectures](#).
- [Building intelligent applications with cognitive APIs \(e-book\)](#).
- [FAQ chatbot architecture](#).

# What is Azure Cognitive Search?

11/9/2020 • 4 minutes to read • [Edit Online](#)

Formerly known as Azure Search, Azure Cognitive Search is a managed cloud solution that gives developers APIs and tools for adding a rich search experience over private, heterogeneous content in web, mobile, and enterprise applications. Your code or a tool invokes data ingestion (indexing) to create and load an index. Optionally, you can add cognitive skills to apply AI processes during indexing. Doing so can add new information and structures that are useful for search and other scenarios.

On the other side of your service, your application code issues query requests and handles responses. The search experience is defined in your client by using functionality from Azure Cognitive Search, with query execution over a persisted index that you create, own, and store in your service.



Functionality is exposed through a simple [REST API](#) or [.NET SDK](#) that masks the inherent complexity of information retrieval. In addition to APIs, the Azure portal provides administration and content management support, with tools for prototyping and querying your indexes. Because the service runs in the cloud, infrastructure and availability are managed by Microsoft.

## When to use Azure Cognitive Search

Azure Cognitive Search is well suited for the following application scenarios:

- Consolidation of heterogeneous content types into a private, single, searchable index. Queries are always over an index that you create and load with documents. The index always resides in the cloud on your Azure Cognitive Search instance. You can populate an index with streams of JSON documents from any source or platform. Alternatively, for content sourced on Azure, you can use an indexer to pull data into an index. Index definition and management/ownership is a key reason for using Azure Cognitive Search.
- Raw content is large undifferentiated text, image files, or application files such as Microsoft Office content types on an Azure data source such as Azure Blob storage or Azure Cosmos DB. You can apply cognitive skills during indexing to add structure or extract meaning from image and application files.
- Easy implementation of search-related features. Azure Cognitive Search APIs simplify query construction, faceted navigation, filters (including geo-spatial search), synonym mapping, type-ahead queries, and relevance tuning. Using built-in features, you can satisfy end-user expectations for a search experience similar to commercial web search engines.
- Indexing unstructured text or extracting text and information from image files. The [AI enrichment](#) feature of Azure Cognitive Search adds AI processing to an indexing pipeline. Some common use cases include OCR over scanned documents, entity recognition and key phrase extraction over large documents, language detection and text translation, and sentiment analysis.
- Linguistic requirements satisfied by using the custom and language analyzers of Azure Cognitive Search. If you have non-English content, Azure Cognitive Search supports both Lucene analyzers and Microsoft's natural

language processors. You can also configure analyzers to achieve specialized processing of raw content, such as filtering out diacritics.

## Use Azure Cognitive Search

### Step 1: Provision the service

You can provision an Azure Cognitive Search instance in the [Azure portal](#) or through the [Azure Resource Manager REST API](#). You can choose either the free service shared with other subscribers or a paid tier that dedicates resources used only by your service. For paid tiers, you can scale a service in two dimensions:

- Add replicas to grow your capacity to handle heavy query loads.
- Add partitions to grow storage for more documents.

By handling document storage and query throughput separately, you can calibrate resourcing based on production requirements.

### Step 2: Create an index

Before you can upload searchable content, you must first define an Azure Cognitive Search index. An index is like a database table that holds your data and can accept search queries. You define the index schema to map to reflect the structure of the documents you want to search, similar to fields in a database.

A schema can be created in the Azure portal or programmatically by using the [.NET SDK](#) or [REST API](#).

### Step 3: Load data

After you define an index, you're ready to upload content. You can use either a push or pull model.

The pull model retrieves data from external data sources. It's supported through indexers that streamline and automate aspects of data ingestion, such as connecting to, reading, and serializing data. [Indexers](#) are available for Azure Cosmos DB, Azure SQL Database, Azure Blob storage, and SQL Server hosted in an Azure Virtual Machines instance. You can configure an indexer for on-demand or scheduled data refresh.

The push model is provided through the SDK or REST APIs used for sending updated documents to an index. You can push data from virtually any dataset by using the JSON format. For more information, see [Add, update, or delete documents](#) or [how to use the .NET SDK](#) for guidance on loading data.

### Step 4: Search

After populating an index, you can [issue search queries](#) to your service endpoint by using simple HTTP requests with [REST APIs](#) or the [.NET SDK](#). Step through [creating your first search application](#) to build and then extend a web page that collects user input and handles results. You can also use [Postman for interactive REST calls](#) or the built-in [Search explorer](#) in the Azure portal to query an existing index.

## Next steps

- Learn more about [Azure Cognitive Search](#).
- Browse more [AI architectures](#).
- See an example knowledge mining solution in the article [JFK Files example architecture and solution](#).

# Innovation in the digital economy

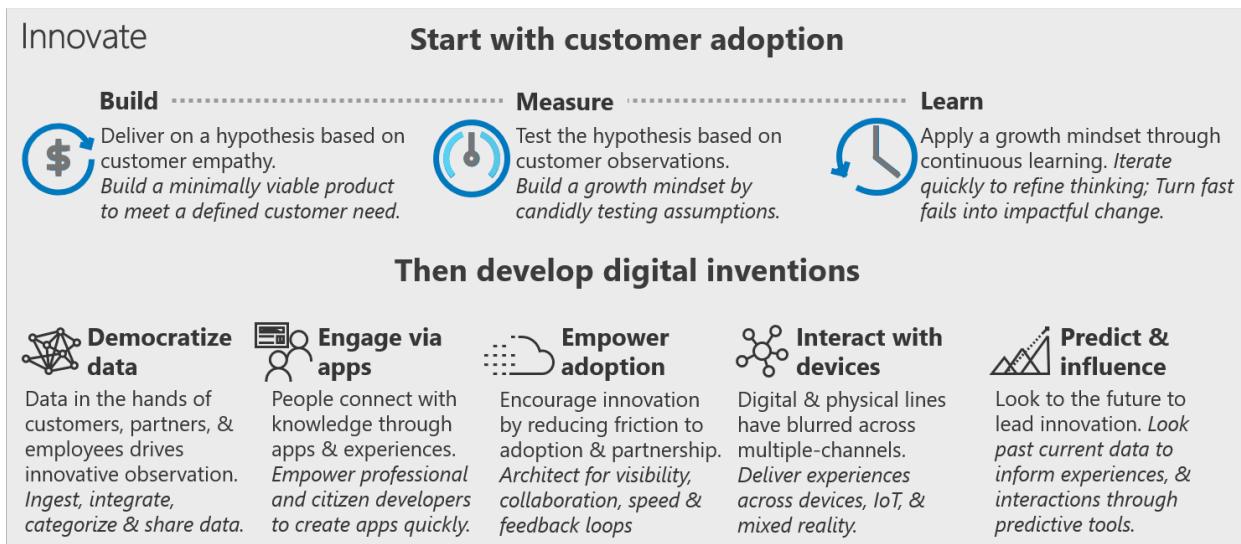
11/9/2020 • 4 minutes to read • [Edit Online](#)

The digital economy is an undeniable force in almost every industry. During the industrial revolution, gasoline, conveyor belts, and human ingenuity were key resources for promoting market innovation. Product quality, price, and logistics drove markets as companies sought to deliver better products to their customers more quickly. Today's digital economy shifts the way in which customers interact with corporations. The primary forms of capital and market differentiators have all shifted as a result. In the digital economy, customers are less concerned with logistics and more concerned with their overall experience of using a product. This shift arises from direct interaction with technology in our daily lives and from a realization of the value associated with those interactions.

In the Innovate methodology of the Cloud Adoption Framework, we'll focus on understanding customer needs and rapidly building innovations that shape how your customers interact with your products. We'll also illustrate an approach to delivering on the value of a minimum viable product (MVP). Finally, we'll map decisions common to innovation cycles to help you understand how the cloud can unlock innovation and create partnerships with your customers.

## Innovate methodology

The simple methodology for cloud innovation within the Cloud Adoption Framework is illustrated in the following image. Subsequent articles in this section will show how to establish core processes, approaches, and mechanisms for finding and driving innovation within your company.



This article series emphasizes the following aspects of this methodology:

- First, always start with customer adoption to generate feedback that builds customer partnerships through the build-measure-learn feedback loop.
- Second, examine approaches to developing digital inventions that prioritize adoption.

The following section describes the formula for innovation and the commitments required for success with this approach.

## Formula for innovation

Successful innovation is not a big-bang transformational event or an elusive magical unicorn. Success in

innovation is more of a balancing act, illustrated by a simple equation: **innovation = invention + adoption**.

Innovation happens at the intersection of invention and adoption. True innovation stems from slowly adjusting human experiences through new approaches, new processes, and new technologies. In this formula, invention means creating a new solution that meets a customer need. Conversely, adoption means applying the new solution to shape human behaviors and interactions. Finding the right balance between invention and adoption requires iteration, data-driven decision making, constant learning, and a growth mindset. It also requires technologies that can keep pace with the countless opportunities to learn in today's digital society.

The cloud is often a great platform for invention or the technological aspects of innovation. Unfortunately, most great ideas fail during the hard work of adoption, rather than during the ideation or invention processes. To ensure success, development teams should always start with adoption as the test for innovation. That's why this methodology starts with adoption. To use this methodology, the following three commitments should be agreed upon by the team:

- [Commitment to prioritize customers over technology](#)
- [Commitment to transparency](#)
- [Commitment to iteration](#)

## Cultural commitments

Adopting the [Innovate methodology](#) requires some cultural commitments to effectively use the metrics outlined in this article. Before you change your approach to driving innovation, make sure the adoption and leadership teams are ready to make these important commitments.

### Commitment to prioritize customers over technology

Every development team has a set of tools or technologies that they're most familiar with. It's wise to play to those strengths and use what you know. However, for innovation to be successful, teams must maintain a focus on customer needs and the hypothesis being tested. At times, this focus may not align with the capabilities of a particular tool or architectural approach. To be successful in innovation, the development team must remain open-minded. During the invention process, focus technical decisions on the needs of the customer over the preferences of your team.

### Commitment to transparency

To understand measurement in an innovation approach, you must first understand the commitment to transparency. Innovation can only thrive in an environment that adheres to a *growth mindset*. At the root of a growth mindset is a cultural imperative to learn from experiences. Successful innovation and continuous learning start with a commitment to transparency in measurement. This is a brave commitment for the cloud adoption team. However, that commitment is meaningless if it's not matched by a commitment to preserve transparency within the leadership and cloud strategy teams.

Transparency is important because measuring customer impact doesn't address the question of right or wrong. Nor are impact measurements indicative of the quality of work or the performance of the adoption team. Instead, they represent an opportunity to learn and better meet your customers' needs. Misuse of innovation metrics can stifle that culture. Eventually, such misuse will lead to manipulation of metrics, which in turn causes long-term failure of the invention, the supporting staff, and ultimately the management structure who misused the data. Leaders and contributors alike should avoid using measurements for anything other than an opportunity to learn and improve the MVP solution.

### Commitment to iteration

Only one promise rings true across all innovation cycles: you won't get it right on the first try. Measurement

helps you understand what adjustments you should make to achieve the desired results. Changes that lead to favorable outcomes stem from iterations of the build-measure-learn process. The cloud adoption team and the cloud strategy team must commit to an iterative mindset before adopting a growth mindset or a build-measure-learn approach.

## Next steps

Before building the next great invention, get started with customer adoption by understanding the [build-measure-learn feedback loop](#).

[Customer adoption with the build-measure-learn feedback loop](#)

# Build consensus on the business value of innovation

11/9/2020 • 5 minutes to read • [Edit Online](#)

The first step to developing any new innovation is to identify how that innovation can drive business value. In this exercise, you answer a series of questions that highlight the importance of investing ample time when your organization defines business value.

## Qualifying questions

Before you develop any solution (in the cloud or on-premises), validate your business value criteria by answering the following questions:

1. What is the defined customer need that you seek to address with this solution?
2. What opportunities would this solution create for your business?
3. Which business outcomes would be achieved with this solution?
4. Which of your company's motivations would be served with this solution?

If the answers to all four questions are well documented, you might not need to complete the rest of this exercise. Fortunately, you can easily test any documentation. Set up two short meetings to test both the documentation and your organization's internal alignment. Invite committed business stakeholders to one meeting and set up a separate meeting with the engaged development team. Ask the four questions above to each group, and then compare the results.

### NOTE

The existing documentation **should not** be shared with either team before the meeting. If true alignment exists, the guiding hypotheses should be referenced or even recited by members of each group.

### WARNING

Don't facilitate the meeting. This test is to determine alignment; it's not an alignment creation exercise. When you start the meeting, remind the attendees that the objective is to test directional alignment to existing agreements within the team. Establish a five-minute time limit for each question. Set a timer and close each question after five minutes even if the attendees haven't agreed upon an answer.

Account for the different languages and interests of each group. If the test results in answers that are directionally aligned, consider this exercise a victory. You're ready to move on to solution development.

If one or two of the answers are directionally aligned, recognize that your hard work is paying off. You're already better aligned than most organizations. Future success is likely with minor continuing investment in alignment. Review each of the following sections for ideas that may help you build further alignment.

If either team fails to answer all four questions in 30 minutes, then alignment and the considerations in the following sections are likely to have a significant impact on this effort and others. Pay careful attention to each of the following sections.

## Address the big picture first

The Cloud Adoption Framework follows a prescribed path through four phases: Strategy, Plan, Ready, and Adopt. Cloud innovation fits within the Adopt phase of this process. The answers to **qualifying questions three and four**

concern outcomes and motivations. When these answers are misaligned, it indicates that your organization missed something during the Strategy phase of the cloud adoption lifecycle. Several of the following scenarios are likely to be at play.

- **Alignment opportunity:** When business stakeholders can't agree on motivations and business outcomes related to a cloud innovation effort, it's a symptom of a larger challenge. The exercises in the [Strategy methodology](#) can be useful in developing alignment among business stakeholders. Additionally, it's highly recommended that the same stakeholders form a [cloud strategy team](#) that meets regularly.
- **Communication opportunity:** When the development team can't agree on motivations and business outcomes, it might be a symptom of strategic communication gaps. You can quickly resolve this issue by reviewing the cloud strategy with the cloud adoption team. Several weeks after the review, the team should repeat the qualifying questions exercise.
- **Prioritization opportunity:** A cloud strategy is essentially an executive-level hypothesis. The best cloud strategies are open to iteration and feedback. If both teams understand the strategy, but still can't quite align answers to these questions, then priorities might be misaligned. Organize a session with the cloud adoption team and the cloud strategy team. This session can help the efforts of both groups. The cloud adoption team starts by sharing their aligned answers to the qualifying questions. From there, a conversation between the cloud adoption team and cloud strategy team can highlight opportunities to better align priorities.

These big picture opportunities often reveal ways to better align the innovative solution with the cloud strategy. This exercise has two common outcomes:

- These conversations can help your team improve your organization's cloud strategy and better represent important customer needs. Such a change can result in greater executive support for your team.
- Conversely, these conversations might show that your cloud adoption team should invest in a different solution. In this case, consider migrating this solution before continuing to invest in innovation. Alternately, these conversations might indicate that you adopt a citizen developer approach to test the business value first. In either case, they will help your team avoid making a large investment with limited business returns.

## Address solution alignment

It's fairly common for the answers to questions one and two to be misaligned. During the early stages of ideation and development, customer need and business opportunity often get out of alignment. Many development teams find it challenging to achieve a balance between too much and too little definition. The Cloud Adoption Framework recommends lean approaches like build-measure-learn feedback loops to answer these questions. The following list shows opportunities and approaches to create alignment.

- **Hypothesis opportunity:** It's common for various stakeholders and development teams to have too many expectations for a solution. Unrealistic expectations can be a sign that the hypothesis is too vague. Follow the guidance on [building with customer empathy](#) to construct a clearer hypothesis.
- **Build opportunity:** Teams might be misaligned because they disagree on the way to solve the customer need. Such disagreement typically indicates that the team is being [delayed by a premature technical spike](#). To keep the team focused on the customer, start the first iteration and build a small minimum viable product (MVP) to address part of the hypothesis. For more guidance to help the team move forward, see [Develop digital inventions](#).
- **Training opportunity:** Either team can be misaligned because they need deep technical requirements and extensive functional requirements. This need can lead to an opportunity for training in agile methodologies. When the team culture isn't ready for agile processes, you might find innovation and keeping pace with the market to be a challenge. For training resources about DevOps and agile practices, see:
  - [Evolve your DevOps practices](#)
  - [Build applications with Azure DevOps](#)

- [Deploy applications with Azure DevOps](#)

By following the methodology and the backlog management tools in each section of this article, you can help create solution alignment.

## Next steps

After you've aligned your business value proposition and communicated it, you're ready to start building your solution.

[Return to the innovate exercises for next steps](#)

# Create customer partnerships through the build-measure-learn feedback loop

11/9/2020 • 2 minutes to read • [Edit Online](#)

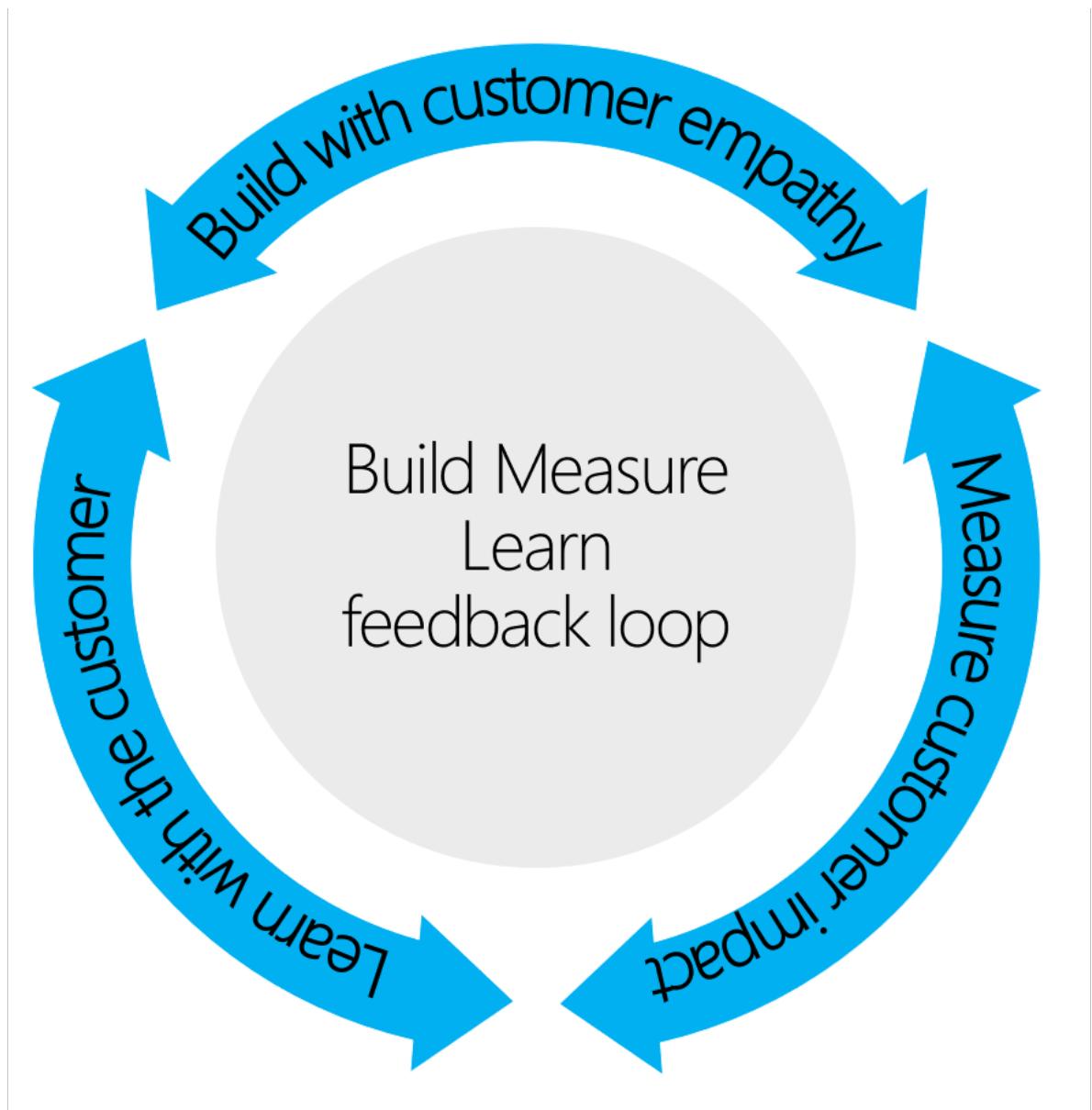
True innovation comes from the hard work of building solutions that demonstrate customer empathy, from measuring the impact of those changes on the customer, and from learning with the customer. Most importantly, it comes from feedback over multiple iterations.

If the past decade has taught us anything about innovation, it's that the old rules of business have changed. Large, wealthy incumbents no longer have an unbreakable hold on the market. The first or best players to market are not always the winners. Having the best idea doesn't lead to market dominance. In a rapidly changing business climate, market leaders are the most agile. Those who can adapt to changing conditions lead.

Large or small, the companies that thrive in the digital economy as innovative leaders are those with the greatest ability to listen to their customer base. That skill can be cultivated and managed. At the core of all good partnerships is a clear feedback loop. The process for building customer partnerships within the Cloud Adoption Framework is the build-measure-learn feedback loop.

## The build-measure-learn feedback loop

As described in [Innovation in the digital economy](#), innovation requires a balance between invention and adoption. Customer feedback and partnership drive adoption. By turning your customers into strong, loyal partners during innovation cycles, you can realize better products and gain quicker traction in the market.



This process for managing customer partnerships and integrating them into your innovation efforts includes three phases of development:

- [Build with customer empathy](#)
- [Measure for customer impact](#)
- [Learn with customers](#)

Each phase of the process helps you build better solutions with your customers.

## Next steps

Learn how to [build with customer empathy](#) to begin your build-measure-learn cycle.

[Build with customer empathy](#)

# Build with customer empathy

11/9/2020 • 11 minutes to read • [Edit Online](#)

"Necessity is the mother of invention." This proverb captures the indelibility of the human spirit and our natural drive to invent. As explained in the Oxford English Dictionary, "When the need for something becomes imperative, you're forced to find ways of getting or achieving it." Few would deny these universal truths about invention. However, as described in [Innovation in the digital economy](#), innovation requires a balance between invention and adoption.

Continuing with the analogy, innovation comes from a more extended family. *Customer empathy is the proud parent of innovation.* creating a solution that drives innovation requires a legitimate customer need that keeps the customer coming back to solve critical challenges. These solutions are based on what a customer needs rather than on their wants or whims. To find their true needs, we start with empathy, a deep understanding of the customer's experience. Empathy is an underdeveloped skill for many engineers, product managers, and even business leaders. Fortunately, the diverse interactions and rapid pace of the cloud architect role have already started fostering this skill.

Why is empathy so important? From the first release of a minimum viable product (MVP) to the general availability of a market-grade solution, customer empathy helps us understand and share in the experience of the customer. Empathy helps us build a better solution. More importantly, it better positions us to invent solutions that will encourage adoption. In a digital economy, those who can most readily empathize with customer needs can build a brighter future that redefines and leads the market.

## How to build with empathy

Defining assumptions is a fundamental part of planning. The more we plan, the more we see assumptions creep into the foundation of a great idea. Assumptions are typically the product of self-empathy. In other words, *what would I want if I were in this position?* Starting with the build phase minimizes the period in which assumptions can invade a solution. This approach also accelerates the feedback loop with real customers, triggering earlier opportunities to learn and sharpen empathy.

### Caution

Properly defining what to build can be tricky and requires some practice. If you build something too quickly, it might not reflect customer needs. If you spend too much time trying to understand initial customer needs and solution requirements, the market may meet them before you have a chance to build anything at all. In either scenario, the opportunity to learn can be significantly delayed or reduced. Sometimes the data can even be corrupted.

The most innovative solutions in history began with an intuitive belief. That gut feeling comes from both existing expertise and firsthand observation. We start with the build phase because it allows for a rapid test of that intuition. From there, we can cultivate deeper understanding and clearer degrees of empathy. At every iteration or release of a solution, balance comes from building MVPs that demonstrate customer empathy.

To steady this balancing act, the following two sections discuss the concepts of building with empathy and defining an MVP.

### Define a customer focused-hypothesis

Building with empathy means creating a solution based on defined hypotheses that illustrate a specific customer need. The following steps aim to formulate a hypothesis that will encourage building with empathy.

1. When you build with empathy, the customer is always the focus. This intention can take many shapes. You could reference a customer archetype, a specific persona, or even a picture of a customer in the midst of the

problem you want to solve. And keep in mind that customers can be internal (employees or partners) or external (consumers or business customers). This definition is the first hypothesis to be tested: can we help this specific customer?

2. Understand the customer experience. Building with empathy means you can relate to the customer's experience and understand their challenges. This mindset indicates the next hypothesis to be tested: can we help this specific customer with this manageable challenge?
3. Define a simple solution to a single challenge. Relying on expertise across people, processes, and subject matter experts will lead to a potential solution. This is the full hypothesis to be tested: can we help this specific customer with this manageable challenge through the proposed solution?
4. Arrive at a value statement. What long-term value do you hope to provide to these customers? The answer to this question creates your full hypothesis: how will these customers' lives be improved by using the proposed solution to address this manageable challenge?

This last step is the culmination of an empathy-driven hypothesis. It defines the audience, the problem, the solution, and the metric by which improvement is to be made, all of which center on the customer. During the measure and learn phases, each hypothesis should be tested. Changes in the customer, problem statement, or solution are anticipated as the team develops greater empathy for the addressable customer base.

**Caution**

The goal is to *build* with customer empathy, not to *plan* with it. It's all too easy to get stuck in endless cycles of planning and tweaking to hit upon the perfect customer empathy statement. Before you try to develop such a statement, review the following sections on defining and building an MVP.

After core assumptions are proven, later iterations will focus on growth tests in addition to empathy tests. After empathy is built, tested, and validated, you can begin to understand the addressable market at scale. This can be done through an expansion of the standard hypothesis formula described earlier. Based on available data, estimate the size of the total market (the number of potential customers).

From there, estimate the percentage of that total market that experiences a similar challenge and that might therefore be interested in this solution. This is your addressable market. The next hypothesis to be tested is: how will  $x\%$  of customers' lives be improved by using the proposed solution to address this manageable challenge? A small sampling of customers will reveal leading indicators that suggest a percentage impact on the pool of customers engaged.

### **Define a solution to test the hypothesis**

During each iteration of a build-measure-learn feedback loop, your attempt to build with empathy is defined by an MVP.

An MVP is the smallest unit of effort (invention, engineering, application development, or data architecture) required to create enough of a solution to learn *with the customer*. The goal of every MVP is to test some or all of the prior hypotheses and to receive feedback directly from the customer. The output is not a beautiful application with all the features required to change your industry. The desired output of each iteration is a learning opportunity, a chance to more deeply test a hypothesis.

*Timeboxing* is a standard way to make sure a product remains lean. For example, make sure your development team thinks the solution can be created in a single iteration to allow for rapid testing. To better understand using velocity, iterations, and releases to define what minimal means, see [Planning velocity, iterations, release, and iteration paths](#).

### **Reduce complexity and delay technical spikes**

The [disciplines of invention](#) found in the [Innovate methodology](#) describe the functionality that's often required to deliver a mature innovation or scale-ready MVP solution. Use these disciplines as a long-term guide for feature inclusion. Likewise, use them as a cautionary guide during early testing of customer value and empathy in your solution.

Feature breadth and the different disciplines of invention can't all be created in a single iteration. It might take several releases for an MVP solution to include the complexity of multiple disciplines. Depending on the investment in development, there might be multiple parallel teams working within different disciplines to test multiple hypotheses. Although it's smart to maintain architectural alignment between those teams, it's unwise to try to build complex, integrated solutions until value hypotheses can be validated.

Complexity is best detected in the frequency or volume of *technical spikes*. Technical spikes are efforts to create technical solutions that can't be easily tested with customers. When customer value and customer empathy are untested, technical spikes represent a risk to innovation and should be minimized. For the types of mature tested solutions found in a migration effort, technical spikes can be common throughout adoption. However, they delay the testing of hypotheses in innovation efforts and should be postponed whenever possible.

A relentless simplification approach is suggested for any MVP definition. This approach means removing anything that doesn't add to your ability to validate the hypothesis. To minimize complexity, reduce the number of integrations and features that aren't required to test the hypothesis.

### **Build an MVP**

At each iteration, an MVP solution can take many different shapes. The common requirement is only that the output allows for measurement and testing of the hypothesis. This simple requirement initiates the scientific process and allows the team to build with empathy. To deliver this customer-first focus, an initial MVP might rely on only one of the [disciplines of invention](#).

In some cases, the fastest path to innovation means temporarily avoiding these disciplines entirely, until the cloud adoption team is confident that the hypothesis has been accurately validated. Coming from a technology company like Microsoft, this guidance might sound counterintuitive. However, this simply emphasizes that customer needs, not a specific technology decision, are the highest priority in an MVP solution.

Typically, an MVP solution consists of a simple application or data solution with minimal features and limited polish. For organizations that have professional development expertise, this path is often the fastest one to learning and iteration. The following list includes several other approaches a team might take to build an MVP:

- A predictive algorithm that's wrong 99 percent of the time but that demonstrates specific desired outcomes.
- An IoT device that doesn't communicate securely at production scale but that demonstrates the value of nearly real-time data within a process.
- An application built by a citizen developer to test a hypothesis or meet smaller-scale needs.
- A manual process that re-creates the benefits of the application to follow.
- A wireframe or video that's detailed enough to allow the customer to interact.

Developing an MVP shouldn't require massive amounts of development investment. Preferably, investment should be as constrained as possible to minimize the number of hypotheses being tested at one time. Then, in each iteration and with each release, the solution is intentionally improved toward a scale-ready solution that represents multiple disciplines of invention.

### **Accelerate MVP development**

Time to market is crucial to the success of any innovation. Faster releases lead to faster learning. Faster learning leads to products that can scale more quickly. At times, traditional application development cycles can slow this process. More frequently, innovation is constrained by limits on available expertise. Budgets, headcount, and availability of staff can all create limits to the number of new innovations a team can handle.

Staffing constraints and the desire to build with empathy have spawned a rapidly growing trend toward citizen developers. These developers reduce risk and provide scale within an organization's professional development community. Citizen developers are subject matter experts where the customer experience is concerned, but they're not trained as engineers. These individuals use prototyping tools or lighter-weight development tools that might be frowned upon by professional developers. These business-aligned developers create MVP solutions and test theories. When aligned well, this process can create production solutions that provide value

but don't pass a sufficiently effective scale hypothesis. They can also be used to validate a prototype before scale efforts begin.

Within any innovate plan, cloud adoption teams should diversify their portfolios to include citizen developer efforts. By scaling development efforts, more hypotheses can be formed and tested at a reduced investment. When a hypothesis is validated and an addressable market is identified, professional developers can harden and scale the solution by using modern development tools.

#### **Final build gate: Customer pain**

When customer empathy is strong, a clearly existing problem should be easy to identify. The customer's pain should be obvious. During build, the cloud adoption team is building a solution to test a hypothesis based on a customer pain point. If the hypothesis is well-defined but the pain point is not, the solution is not truly based on customer empathy. In this scenario, build is not the right starting point. Instead, invest first in building empathy and learning from real customers. The best approach for building empathy and validating pain is simple: listen to your customers. Invest time in meeting with and observing them until you can identify a pain point that occurs frequently. After the pain point is well-understood, you're ready to test a hypothesized solution for addressing that pain.

## When not to apply this approach

Many legal, compliance, and industry requirements that might necessitate an alternate approach. If public releases of a developing solution create risk to patent timing, intellectual property protection, customer data leaks, or violation of established compliance requirements, this approach may not be suitable. When perceived risks like these exist, consult legal counsel before adopting any guided approach to release management.

## References

Some of the concepts in this article build on topics discussed in [The Lean Startup](#) by Eric Ries.

## Next steps

After you've built an MVP solution, you can measure the empathy value and scale value. Learn how to [measure for customer impact](#).

[Measure for customer impact](#)

# Measure for customer impact

11/9/2020 • 4 minutes to read • [Edit Online](#)

There are several ways to measure for customer impact. This article will help you define metrics to validate hypotheses that arise out of an effort to [build with customer empathy](#).

## Strategic metrics

The [Strategy methodology](#) examines [motivations](#) and [business outcomes](#). These practices provide a set of metrics to test customer impact. When innovation is successful, you'll usually see results that are aligned with your strategic objectives.

Before establishing learning metrics, define a small number of strategic metrics that you want this innovation to affect. Generally, those strategic metrics align with one or more of the following outcome areas:

- [Business agility](#)
- [Customer engagement](#)
- [Customer reach](#)
- [Financial impact](#)
- [Solution performance](#), in the case of operational innovation.

Document the agreed-upon metrics and track their impact frequently, but don't expect results in any of these metrics to emerge for several iterations. For more information about setting and aligning expectations across the parties involved, see [Commitment to iteration](#).

Aside from motivation and business outcome metrics, the remainder of this article focuses on learning metrics designed to guide transparent discovery and customer-focused iterations. For more information about these aspects, see [Commitment to transparency](#).

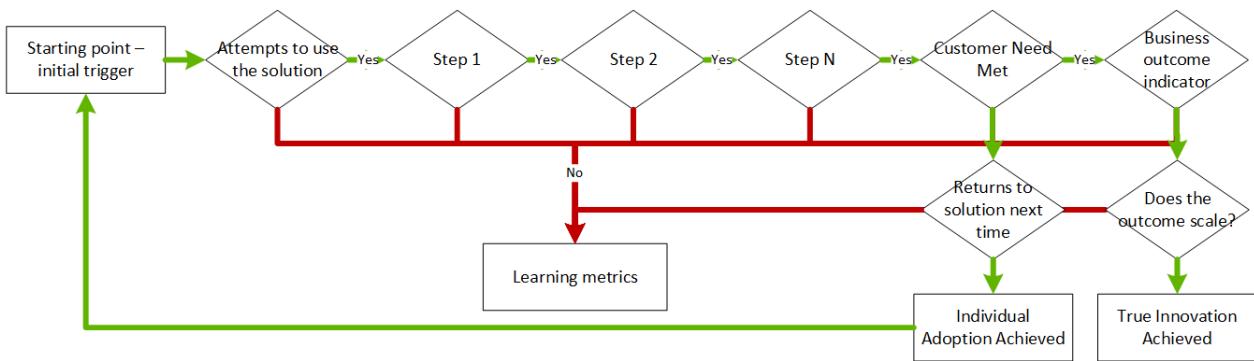
## Learning metrics

When the first version of any minimum viable product (MVP) is shared with customers, preferably at the end of the first development iteration, there will be no impact on strategic metrics. Several iterations later, the team may still be struggling to change behaviors enough to materially affect strategic metrics. During learning processes, such as build-measure-learn cycles, we advise the team to adopt learning metrics. These metrics tracking and learning opportunities.

### **Customer flow and learning metrics**

If an MVP solution validates a customer-focused hypothesis, the solution will drive some change in customer behaviors. Those behavior changes across customer cohorts should improve business outcomes. Keep in mind that changing customer behavior is typically a multistep process. Because each step provides an opportunity to measure impact, the adoption team can keep learning along the way and build a better solution.

Learning about changes to customer behavior starts by mapping the flow that you hope to see from an MVP solution.



In most cases, a customer flow will have an easily defined starting point and no more than two endpoints. Between the start and endpoints are a variety of learning metrics to be used as measures in the feedback loop:

1. **Starting point—initial trigger:** The starting point is the scenario that triggers the need for this solution. When the solution is built with customer empathy, that initial trigger should inspire a customer to try the MVP solution.
2. **Customer need met:** The hypothesis is validated when a customer need has been met by using the solution.
3. **Solution steps:** This term refers to the steps that are required to move the customer from the initial trigger to a successful outcome. Each step produces a learning metric based on a customer decision to move on to the next step.
4. **Individual adoption achieved:** The next time the trigger is encountered, if the customer returns to the solution to get their need met, individual adoption has been achieved.
5. **Business outcome indicator:** When a customer behaves in a way that contributes to the defined business outcome, a business outcome indicator is observed.
6. **True innovation:** When *business outcome indicators* and *individual adoption* both occur at the desired scale, you've realized true innovation.

Each step of the customer flow generates learning metrics. After each iteration (or release), a new version of the hypothesis is tested. At the same time, tweaks to the solution are tested to reflect adjustments in the hypothesis. When customers follow the prescribed path in any given step, a positive metric is recorded. When customers deviate from the prescribed path, a negative metric is recorded.

These alignment and deviation counters create learning metrics. Each should be recorded and tracked as the cloud adoption team progresses toward business outcomes and true innovation. In [Learn with customers](#), we'll discuss ways to apply these metrics to learn and build better solutions.

### Group and observe customer partners

The first measurement in defining learning metrics is the customer partner definition. Any customer who participates in innovation cycles qualifies as a customer partner. To accurately measure behavior, you should use a cohort model to define customer partners. In this model, customers are grouped to sharpen your understanding of their responses to changes in the MVP. These groups typically resemble the following:

- **Experiment or focus group:** Grouping customers based on their participation in a specific experiment designed to test changes over time.
- **Segment:** Grouping customers by the size of the company.
- **Vertical:** Grouping customers by the *industry vertical* they represent.
- **Individual demographics:** Grouping based on personal demographics like age and physical location.

These types of groupings help you validate learning metrics across various cross-sections of those customers who choose to partner with you during your innovation efforts. All subsequent metrics should be derived from definable customer grouping.

## Next steps

As learning metrics accumulate, the team can begin to [learn with customers](#).

### Learn with customers

Some of the concepts in this article build on topics first described in [The Lean Startup](#), written by Eric Ries.

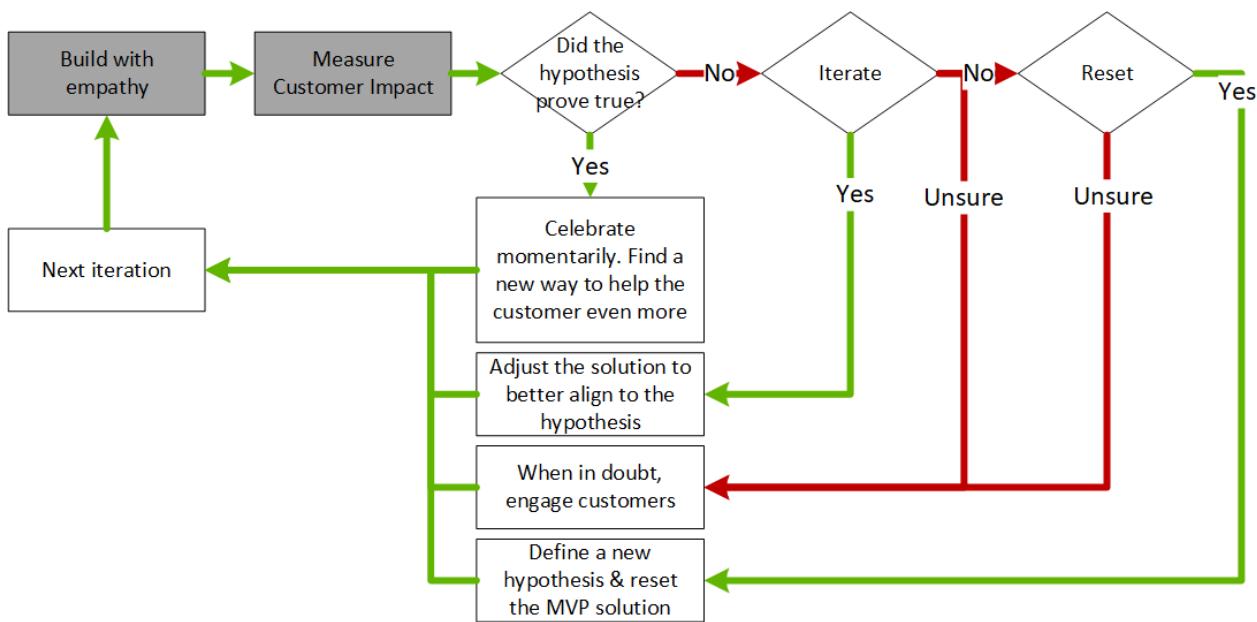
# Learn with customers

11/9/2020 • 4 minutes to read • [Edit Online](#)

Our current customers represent our best resource for learning. By partnering with us, they help us [build with customer empathy](#) to find the best solution to their needs. They also help create a minimum viable product (MVP) solution by generating metrics from which we [measure customer impact](#). In this article, we'll describe how to learn with and from our customer-partners.

## Continuous learning

At the end of every iteration, we have an opportunity to learn from the build and measure cycles. This process of continuous learning is quite simple. The following image offers an overview of the process flow.



At its most basic, continuous learning is a method for responding to learning metrics and assessing their impact on customer needs. This process consists of three primary decisions to be made at the end of each iteration:

- **Did the hypothesis prove true?** When the answer is yes, celebrate for a moment and then move on. There are always more things to learn, more hypotheses to test, and more ways to help the customer in your next iteration. When a hypothesis proves true, it's often a good time for teams to decide on a new feature that will enhance the solution's utility for the customer.
- **Can you get closer to a validated hypothesis by iterating on the current solution?** The answer is usually yes. Learning metrics typically suggest points in the process that lead to customer deviation. Use these data points to find the root of a failed hypothesis. At times, the metrics may also suggest a solution.
- **Is a reset of the hypothesis required?** The scariest thing to learn in any iteration is that the hypothesis or underlying need was flawed. When this happens, an iteration alone isn't necessarily the right answer. When a reset is required, the hypothesis should be rewritten and the solution reviewed in light of the new hypothesis. The sooner this type of learning occurs, the easier it will be to pivot. Early hypotheses should focus on testing the riskiest aspects of the solution in service of avoiding pivots later in development.
- **Unsure?** The second most common response after "iterate" is "we're not sure." Embrace this response. It represents an opportunity to engage the customer and to look beyond the data.

The answers to these questions will shape the iteration to follow. Companies that demonstrate an ability to apply continuous learning and boldly make the right decisions for their customers are more likely to emerge as leaders

in their markets.

For better or worse, the practice of continuous learning is an art that requires a great deal of trial and error. It also requires some science and data-driven decision-making. Perhaps the most difficult part of adopting continuous learning concerns the cultural requirements. To effectively adopt continuous learning, your business culture must be open to a fail first, customer-focused approach. The following section provides more details about this approach.

## Growth mindset

Few could deny the radical transformation within Microsoft culture that's occurred over the last several years. This multifaceted transformation, led by Satya Nadella, has been hailed as a surprising business success story. At the heart of this story is the simple belief we call the growth mindset. An entire section of this framework could be dedicated to the adoption of a growth mindset. But to simplify this guidance, we'll focus on a few key points that inform the process of learning with customers:

- **Customer first:** If a hypothesis is designed to improve the experience of real customers, you have to meet real customers where they are. Don't just rely on metrics. Compare and analyze metrics based on firsthand observation of customer experiences.
- **Continuous learning:** Customer focus and customer empathy stem from a learn-it-all mindset. The Innovate methodology strives to be learn-it-all, not know-it-all.
- **Beginner's mindset:** Demonstrate empathy by approaching every conversation with a beginner's mindset. Whether you're new to your field or a 30-year veteran, assume you know little, and you'll learn a lot.
- **Listen more:** Customers want to partner with you. Unfortunately, an ego-driven need to be right blocks that partnership. To learn beyond the metrics, speak less and listen more.
- **Encourage others:** Don't just listen; use the things you **do** say to encourage others. In every meeting, find ways to pull in diverse perspectives from those who may not be quick to share.
- **Share the code:** When we feel our obligation is to the ownership of a code base, we lose sight of the true power of innovation. Focus on owning and driving outcomes for your customers. Share your code (publicly with the world or privately within your company) to invite diverse perspectives into the solution and the code base.
- **Challenge what works:** Success doesn't necessarily mean you're demonstrating true customer empathy. Avoid having a fixed mindset and a bias toward doing what's worked before. Look for learning in positive and negative metrics by engaging your customers.
- **Be inclusive:** Work hard to invite diverse perspectives into the mix. There are many variables that can divide humans into segregated groups. Cultural norms, past behaviors, gender, religion, sexual preference, even physical abilities. True innovation comes when we challenge ourselves to see past our differences and consciously strive to include all customers, partners, and coworkers.

## Next steps

As a next step to understanding this methodology, see [Common blockers and challenges to innovation](#) to prepare for the changes ahead.

### [Understanding common blockers and challenges](#)

Some of the concepts in this article build on topics first described in [The Lean Startup](#), written by Eric Ries.

# Common blockers and challenges to innovation

11/9/2020 • 5 minutes to read • [Edit Online](#)

As described in [Innovation in the digital economy](#), innovation requires a balance between invention and adoption. This article expands on the common challenges and blockers to innovation, as it aims to help you understand how this approach can add value during your innovation cycles. Formula for innovation: **innovation = invention + adoption**

## Adoption challenges

Cloud technology advances have reduced some of the friction related to adoption. However, adoption is more people-centric than technology-centric. And unfortunately, the cloud can't fix people.

The following list elaborates on some of the most common adoption challenges related to innovation. As you progress through the Innovate methodology, each of the challenges in the following sections will be identified and addressed. Before you apply this methodology, evaluate your current innovation cycles to determine which are the most important challenges or blockers for you. Then, use the methodology to address or remove those blockers.

### External challenges

- **Time to market:** In a digital economy, time to market is one of the most crucial indicators of market domination. Surprisingly, time to market impact has little to do with positioning or early market share. Both of those factors are fickle and temporary. The time to market advantage comes from the simple truth that more time your solution has on the market, the more time you have to learn, iterate, and improve. Focus heavily on quick definition and rapid build of an effective minimum viable product to shorten time to market and accelerate learning opportunities.
- **Competitive challenges:** Dominant incumbents reduce opportunities to engage and learn from customers. Competitors also create external pressure to deliver more quickly. Build fast but invest heavily in understanding the proper *measures*. Well-defined niches produce more actionable feedback measures and enhance your ability to partner and learn, resulting in better overall solutions.
- **Understand your customer:** Customer empathy starts with an understanding of the customer and customer base. One of the biggest challenges for innovators is the ability to rapidly categorize measurements and learning within the build-measure-learn cycle. It's important to understand your customer through the lenses of market segmentation, channels, and types of relationships. Throughout the build-measure-learn cycle, these data points help create empathy and shape the lessons learned.

### Internal challenges

- **Choosing innovation candidates:** When investing in innovation, healthy companies spawn an endless supply of potential inventions. Many of these create compelling business cases that suggest high returns and generate enticing business justification spreadsheets. As described in the build article, *building with customer empathy* should be prioritized over invention that's based only on gain projections. If customer empathy isn't visible in the proposal, long-term adoption is unlikely.
- **Balancing the portfolio:** Most technology implementations don't focus on changing the market or improving the lives of customers. In the average IT department, more than 80% of workloads are maintained for basic process automation. With the ease of innovation, it's tempting to innovate and rearchitect those solutions. Most of the times, those workloads can experience similar or better returns by migrating or modernizing the solution, with no change to core business logic or data processes. Balance your portfolio to favor innovation strategies that can be *built* with clear empathy for the customer (internal or external). For all other workloads, follow a migrate path to financial returns.
- **Maintaining focus and protecting priorities:** When you've made a commitment to innovation, it's

important to maintain your team's focus. During the first iteration of a build phase, it's relatively easy to keep a team excited about the possibilities of changing the future for your customers. However, that first MVP release is just the beginning. True innovation comes with each build-measure-learn cycle, by learning from the feedback loops to produce a better solution. As a leader in any innovation process, you should concentrate on keeping the team focused and on maintaining your innovation priorities through the subsequent, less-glamorous build iterations.

## Invention challenges

Before the widespread adoption of the cloud, invention cycles that depended on information technology were laborious and time-consuming. Procurement and provisioning cycles frequently delayed the crucial first steps toward any new solutions. The cost of DevOps solutions and feedback loops delayed teams' abilities to collaborate on early stage ideation and invention. Costs related to developer environments and data platforms prevented anyone but highly trained professional developers from participating in the creation of new solutions.

The cloud has overcome many of these invention challenges by providing self-service automated provisioning, light-weight development and deployment tools, and opportunities for professional developers and citizen developers to cooperate in creating rapid solutions. Using the cloud for innovation dramatically reduces customer challenges and blockers to the invention side of the innovation equation.

### Invention challenges in a digital economy

The invention challenges of today are different. The endless potential of cloud technologies also produces more implementation options and deeper considerations about how those implementations might be used.

The Innovate methodology uses the following innovation disciplines to help align your implementation decisions with your invention and adoption goals:

- **Data platforms:** New sources and variations on data are available. Many of these couldn't be integrated into legacy or on-premises applications to create cost-effective solutions. Understanding the change you hope to drive in customers will inform your data platform decisions. Those decisions will be an extension of selected approaches to ingest, integrate, categorize, and share data. Microsoft refers to this decision-making process as the democratization of data.
- **Device interactions:** IoT, mobile, and augmented reality blur the lines between digital and physical, accelerating the digital economy. Understanding the real-world interactions surrounding customer behavior will drive decisions about device integration.
- **Applications:** Applications are no longer the exclusive domain of professional developers. Nor do they require traditional server-based approaches. Empowering professional developers, enabling business specialists to become citizen developers, and expanding compute options for API, micro-services, and PaaS solutions expand application interface options. Understanding the digital experience required to shape customer behavior will improve your decision-making about application options.
- **Source code and deployment:** Collaboration between developers of all walks improves both quality and speed to market. Integration of feedback and a rapid response to learning shape market leaders. Commitments to the build, measure, and learn processes help accelerate tool adoption decisions.
- **Predictive solutions:** In a digital economy, it's seldom sufficient to simply meet the current needs of your customers. Customers expect businesses to anticipate their next steps and predict their future needs. Continuous learning often evolves into prediction tooling. The complexity of customer needs and the availability of data will help define the best tools and approaches to predict and influence.

In a digital economy, the greatest challenge architects face is to clearly understand their customers' invention and adoption needs and to then determine the best cloud-based toolchain to deliver on those needs.

## Next steps

With the knowledge you've gained about the build-measure-learn model and a growth mindset, you're ready to

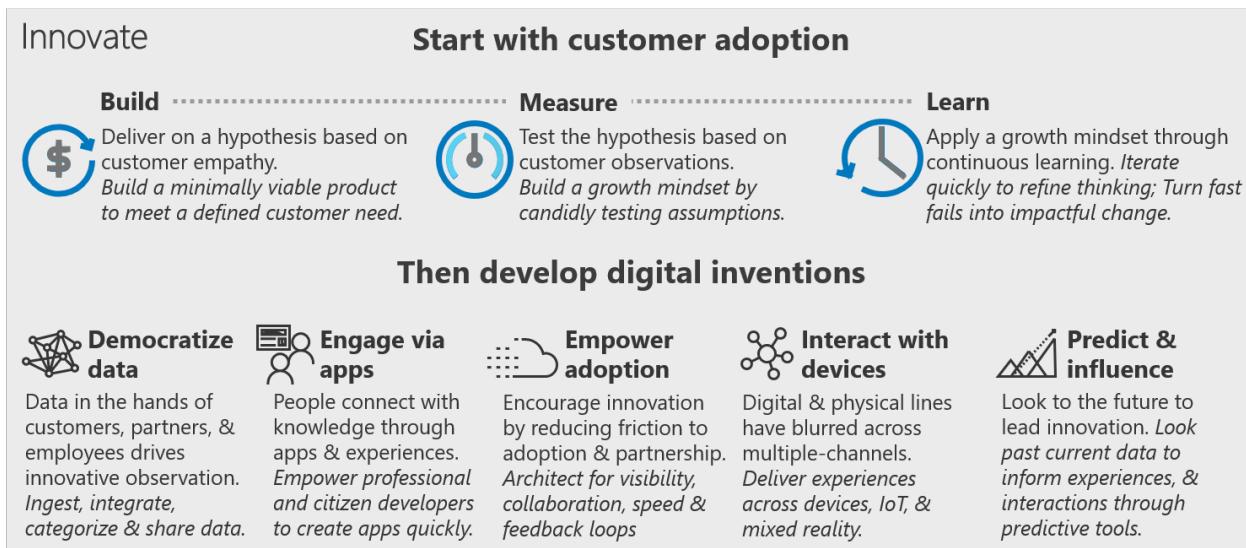
develop digital inventions within the [Innovate methodology](#).

Develop digital inventions

# Develop digital inventions

11/9/2020 • 2 minutes to read • [Edit Online](#)

As described in [Innovation in the digital economy](#), innovation requires a balance between invention and adoption. Customer feedback and partnership are required to drive adoption. The disciplines described in the next section define a series of approaches to developing digital inventions while keeping adoption and customer empathy in mind. Each of the disciplines is briefly described, along with deeper links into each process.



## Summary of each discipline of digital invention

Not every discipline is required to drive innovation for each specific case. By following the guidance in [Build with customer empathy](#), the objective is to test a hypothesis in every iteration. By defining the output of each iteration as a [minimum viable product \(MVP\)](#), this should enable you to involve the fewest possible number of disciplines.

- **Democratize data**: By getting data into the hands of customers, partners, and employees, you encourage innovative observation. Ingest, centralize, govern, and share data.
- **Engage via applications**: People connect with knowledge through applications and experiences. Empower professional and citizen developers to create applications quickly.
- **Empower adoption**: Encourage innovation by reducing friction to adoption and partnership. Architect for visibility, collaboration, speed, and feedback loops.
- **Interact with devices**: Digital and physical lines have blurred across multiple-channels. Deliver experiences across devices, IoT, and mixed reality.
- **Predict and influence**: Look to the future to lead innovation. Look past current data to inform experiences and interactions through predictive tools.

## Next steps

[Democratization of data](#) is the first discipline of innovation to consider and evaluate.

[Democratize data](#)

# Democratize data with digital invention

11/9/2020 • 7 minutes to read • [Edit Online](#)

Coal, oil, and human potential were the three most consequential assets during the industrial revolution. These assets built companies, shifted markets, and ultimately changed nations. In the digital economy, there are three equally important assets: data, devices, and human potential. Each of these assets holds great innovation potential. For any innovation effort in the modern era, data is the new oil.

Across every company today, there are pockets of data that could be used to find and meet customer needs more effectively. Unfortunately, the process of mining that data to drive innovation has long been costly and time-consuming. Many of the most valuable solutions to customer needs go unmet because the right people can't access the data they need.

Democratization of data is the process of getting this data into the right hands to drive innovation. This process can take several forms, but they generally include solutions for ingested or integrated raw data, centralization of data, sharing data, and securing data. When these methods are successful, experts around the company can use the data to test hypotheses. In many cases, cloud adoption teams can [build with customer empathy](#) using only data, and rapidly addressing existing customer needs.

## Process of democratizing data

The following phases will guide the decisions and approaches required to adopt a solution that democratizes data. Not every phase will necessarily be required to build a specific solution. However, you should evaluate each phase when you're building a solution to a customer hypothesis. Each provides a unique approach to the creation of innovative solutions.



### Share data

When you [build with customer empathy](#), all processes elevate customer need over a technical solution. Because democratizing data is no exception, we start by sharing data. To democratize data, it must include a solution that shares data with a data consumer. The data consumer could be a direct customer or a proxy who makes decisions for customers. Approved data consumers can analyze, interrogate, and report on centralized data, with no support from IT staff.

Many successful innovations have been launched as a minimum viable product (MVP) that deliver manual, data-driven processes on behalf of the customer. In this concierge model, an employee is the data consumer. That employee uses data to aid the customer. Each time the customer engages manual support, a hypothesis can be tested and validated. This approach is often a cost effective means of testing a customer-focused hypothesis before you invest heavily in integrated solutions.

The primary tools for sharing data directly with data consumers include self-service reporting or data embedded within other experiences, using tools like [Power BI](#).

## NOTE

Before you share data, make sure you've read the following sections. Sharing data might require governance to provide protection for the shared data. Also, that data might be spread across multiple clouds and could require centralization. Much of the data might even reside within applications, which will require data collection before you can share it.

## Govern data

Sharing data can quickly produce an MVP that you can use in customer conversations. However, to turn that shared data into useful and actionable knowledge, a bit more is generally required. After a hypothesis has been validated through data sharing, the next phase of development is typically data governance.

Data governance is a broad topic that could require its own dedicated framework. That degree of granularity is outside the scope of the [Cloud Adoption Framework](#). However, there are several aspects of data governance that you should consider as soon as the customer hypothesis is validated. For example:

- **Is the shared data sensitive?** Data should be [classified](#) before being shared publicly to protect the interests of customers and the company.
- **If the data is sensitive, has it been secured?** Protection of sensitive data should be a requirement for any democratized data. The example workload focused on [securing data solutions](#) provides a few references for securing data.
- **Is the data cataloged?** Capturing details about the data being shared will aid in long-term data management. Tools for documenting data, like Azure Data Catalog, can make this process much easier in the cloud. Guidance regarding the [annotation of data](#) and the [documentation of data sources](#) can help accelerate the process.

When democratization of data is important to a customer-focused hypothesis, make sure the governance of shared data is somewhere in the release plan. This will help protect customers, data consumers, and the company.

## Centralize data

When data is disrupted across an IT environment, opportunities to innovate can be extremely constrained, expensive, and time-consuming. The cloud provides new opportunities to centralize data across data silos. When centralization of multiple data sources is required to [build with customer empathy](#), the cloud can accelerate the testing of hypotheses.

### Caution

Centralization of data represents a risk point in any innovation process. When data centralization is a [technical spike](#), and not a source of customer value, we suggest that you delay centralization until the customer hypotheses have been validated.

If centralization of data is required, you should first define the appropriate data store for the centralized data. It's a good practice to establish a data warehouse in the cloud. This scalable option provides a central location for all your data. This type of solution is available in online analytical processing (OLAP) or big data options.

The reference architectures for [OLAP](#) and [big data](#) solutions can help you choose the most relevant solution in Azure. If a hybrid solution is required, the reference architecture for [extending on-premises data](#) can also help accelerate solution development.

## IMPORTANT

Depending on the customer need and the aligned solution, a simpler approach may be sufficient. The cloud architect should challenge the team to consider lower cost solutions that could result in faster validation of the customer hypothesis, especially during early development. The following section on collecting data covers some scenarios that might suggest a different solution for your situation.

## Collect data

When you need data to be centralized to address a customer need, it's very likely that you'll also have to collect the data from various sources and move it into the centralized data store. The two primary forms of data collection are *integration* and *ingestion*.

**Integration:** Data that resides in an existing data store can be integrated into the centralized data store by using traditional data movement techniques. This is especially common for scenarios that involve multicloud data storage. These techniques involve extracting the data from the existing data store and then loading it into the central data store. At some point in this process, the data is typically transformed to be more usable and relevant in the central store.

Cloud-based tools have turned these techniques into pay-per-use tools, reducing the barrier to entry for data collection and centralization. Tools like Azure Database Migration Service and Azure Data Factory are two examples. The reference architecture for [data factory with an OLAP data store](#) is an example of one such solution.

**Ingestion:** Some data doesn't reside in an existing data store. When this transient data is a primary source of innovation, you'll want to consider alternative approaches. Transient data can be found in a variety of existing sources like applications, APIs, data streams, IoT devices, a blockchain, an application cache, in media content, or even in flat files.

You can integrate these various forms of data into a central data store on an OLAP or big data solution. However, for early iterations of the build-measure-learn cycle, an online transactional processing (OLTP) solution might be more than sufficient to validate a customer hypothesis. OLTP solutions aren't the best option for any reporting scenario. However, when you're [building with customer empathy](#), it's more important to focus on customer needs than on technical tooling decisions. After the customer hypothesis is validated at scale, a more suitable platform might be required. The reference architecture on [OLTP data stores](#) can help you determine which data store is most appropriate for your solution.

**Virtualize:** Integration and ingestion of data can sometimes slow innovation. When a solution for data virtualization is already available, it might represent a more reasonable approach. Ingestion and integration can both duplicate storage and development requirements, add data latency, increase attack surface area, trigger quality issues, and increase governance efforts. Data virtualization is a more contemporary alternative that leaves the original data in a single location and creates pass-through or cached queries of the source data.

SQL Server 2017 and Azure SQL Data Warehouse both support [PolyBase](#), which is the approach to data virtualization most commonly used in Azure.

## Next steps

With a strategy for democratizing data in place, you'll next want to evaluate approaches to [engaging customers through applications](#).

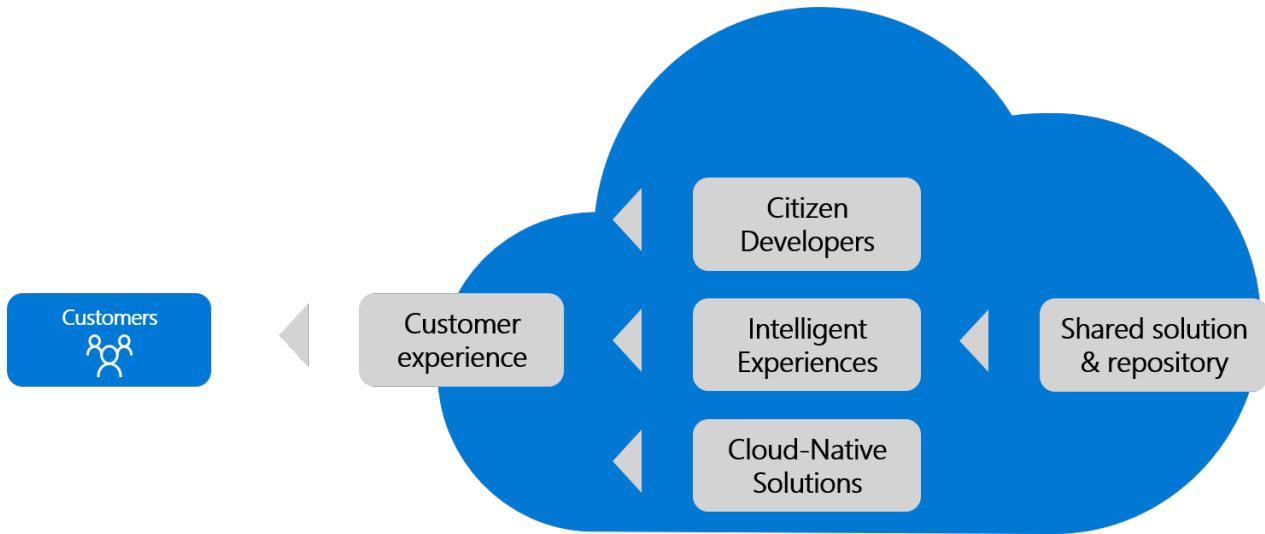
[Engaging customers through applications](#)

# Engage via applications

11/9/2020 • 8 minutes to read • [Edit Online](#)

As discussed in [Democratize data](#), data is the new oil. It fuels most innovations across the digital economy. Building on that analogy, applications are the fueling stations and infrastructure required to get that fuel into the right hands.

In some cases, data alone is enough to drive change and meet customer needs. More commonly though, solutions to customer needs require applications to shape the data and create an experience. Applications are the way we engage the user and the home for the processes required to respond to customer triggers. Applications are how customers provide data and receive guidance. This article summarizes several principles that can help align you with the right application solution, based on the hypotheses to be validated.



## Shared code

Teams that more quickly and accurately respond to customer feedback, market changes, and opportunities to innovate typically lead their respective markets in innovation. The first principle of innovative applications is summed up in the [growth mindset overview](#): "Share the code." Over time, innovation emerges from a cultural focus. To sustain innovation, diverse perspectives and contributions are required.

To be ready for innovation, all application development should start with a shared code repository. The most widely adopted tool for managing code repositories is [GitHub](#), which allows you to create a shared code repository quickly. Alternatively, [Azure Repos](#) is a set of version control tools in Azure DevOps Services that you can use to manage your code. Azure Repos provides two types of version control:

- [Git](#): Distributed version control.
- [Team Foundation Version Control \(TFVC\)](#): Centralized version control.

## Citizen developers

Professional developers are a vital component of innovation. When a hypothesis proves accurate at scale, professional developers are required to stabilize and prepare the solution for scale. Most of the principles referenced in this article require support from professional developers. Unfortunately, current trends suggest there's a greater demand for professional developers than there are developers. Moreover, the cost and pace of innovation can be less favorable when professional development is deemed necessary. In response to these challenges, citizen developers provide a way to scale development efforts and accelerate early hypothesis testing.

The use of citizen developers can be viable and effective when early hypotheses can be validated through tools like [Power Apps](#) for application interfaces, [AI Builder](#) for processes and predictions, [Microsoft Power Automate](#) for workflows, and [Power BI](#) for data consumption.

#### **NOTE**

When you rely on citizen developers to test hypotheses, it's advisable to have some professional developers on hand to provide support, review, and guidance. After a hypothesis is validated at scale, a process for transitioning the application into a more robust programming model will accelerate returns on the innovation. By involving professional developers in process definitions early on, you can realize cleaner transitions later.

## Intelligent experiences

Intelligent experiences combine the speed and scale of modern web applications with the intelligence of Cognitive Services and bots. Alone, each of these technologies might be sufficient to meet your customers' needs. When smartly combined, they broaden the spectrum of needs that can be met through a digital experience, while helping to contain development costs.

### **Modern web apps**

When an application or experience is required to meet a customer need, modern web applications can be the fastest way to go. Modern web experiences can engage internal or external customers quickly and allow for rapid iteration on the solution.

### **Infusing intelligence**

Machine learning and AI are increasingly available to developers. The wide-spread availability of common APIs with predictive capabilities allows developers to better meet the needs of the customer through expanded access to data and predictions.

Adding intelligence to a solution can enable speech to text, text translation, Computer Vision, and even visual search. With these expanded capabilities, it's easier for developers to build solutions that take advantage of intelligence to create an interactive and modern experience.

### **Bots**

Bots provide an experience that feels less like using a computer and more like dealing with a person — at least with an intelligent robot. They can be used to shift simple, repetitive tasks (such as making a dinner reservation or gathering profile information) onto automated systems that might no longer require direct human intervention. Users converse with a bot through text, interactive cards, and speech. A bot interaction can range from a quick question-and-answer to a sophisticated conversation that intelligently provides access to services.

Bots are a lot like modern web applications: they live on the internet and use APIs to send and receive messages. What's in a bot varies widely depending on what kind of bot it is. Modern bot software relies on a stack of technology and tools to deliver increasingly complex experiences on a variety of platforms. However, a simple bot could just receive a message and echo it back to the user with very little code involved.

Bots can do the same things as other types of software: read and write files, use databases and APIs, and handle regular computational tasks. What makes bots unique is their use of mechanisms generally reserved for human-to-human communication.

## Cloud-native solutions

Cloud-native applications are built from the ground up, and they're optimized for cloud scale and performance. Cloud-native applications are typically built using a microservices, serverless, event-based, or container-based approaches. Most commonly, cloud-native solutions use a combination of microservices architectures, managed services, and continuous delivery to achieve reliability and faster time to market.

A cloud-native solution allows centralized development teams to maintain control of the business logic without the need for monolithic, centralized solutions. This type of solution also creates an anchor to drive consistency across the input of citizen developers and modern experiences. Finally, cloud-native solutions provide an innovation accelerator by freeing citizen and professional developers to innovate safely and with a minimum of blockers.

## Innovate through existing solutions

Many customer hypotheses can best be delivered by a modernized version of an existing solution. When the current business logic meets customer needs (or comes really close), you might be able to accelerate innovation by building on top of a modernized solution.

Most forms of modernization, including slight refactoring of the application, are included in the [Migrate methodology](#) within the Cloud Adoption Framework. That methodology guides cloud adoption teams through the process of migrating a [digital estate](#) to the cloud. The [Azure migration guide](#) provides a streamlined approach to the same methodology, which is suitable for a small number of workloads or even a single application.

After a solution has been migrated and modernized, there are a variety of ways it can be used to create new, innovative solutions to customer needs. For example, [citizen developers](#) could test hypotheses, or professional developers could create [intelligent experiences](#) or [cloud-native solutions](#).

### Extend an existing solution

Extending a solution is one common form of modernization. This approach can be the fastest path to innovation when the following are true of the customer hypothesis:

- Existing business logic should meet (or comes close to meeting) the existing customer need.
- An improved experience would better meet the needs of a specific customer cohort.
- The business logic required by the minimum viable product (MVP) solution has been centralized, usually via an [n-tier](#), web services, API, or [microservices](#) design. This approach consists of wrapping the existing solution within a new experience hosted in the cloud. In Azure, this solution would likely live in Azure App Service.

### Rebuild an existing solution

If an application can't be easily extended, it may be necessary to refactor the solution. In this approach, the workload is migrated to the cloud. After the application is migrated, parts of it are modified or duplicated, as web services or [microservices](#), which are deployed in parallel with the existing solution. The parallel service-based solution could be treated like an extended solution. This solution would simply wrap the existing solution with a new experience hosted in the cloud. In Azure, this solution would likely live in Azure App Service.

#### Caution

Refactoring or rearchitecting solutions or centralizing business logic can quickly trigger a time-consuming [technical spike](#) instead of a source of customer value. This is a risk to innovation, especially early in hypothesis validation. With a bit of creativity in the design of a solution, there should be a path to MVP that doesn't require refactoring of existing solutions. It's wise to delay refactoring until the initial hypothesis can be validated at scale.

## Operating model innovations

In addition to modern innovative approaches to application creation, there have been notable innovations in application operations. These approaches have spawned many organizational movements. One of the most prominent is the [cloud center of excellence](#) operating model. When fully staffed and mature, business teams have the option to provide their own operational support for a solution.

The type of self-service operational management model found in a cloud center of excellence allows for tighter controls and faster iterations within the solution environment. These goals are accomplished by transferring operational control and accountability to the business team.

If you're trying to scale or meet global demand for an existing solution, this approach might be sufficient to

validate a customer hypothesis. After a solution is migrated and slightly modernized, the business team can scale it to test a variety of hypotheses. These typically involve customer cohorts who are concerned with performance, global distribution, and other customer needs hindered by IT operations.

## Reduce overhead and management

The more there is to maintain within a solution, the slower that solution will iterate. This means you can accelerate innovation by reducing the impact of operations on available bandwidth.

To prepare for the many iterations required to deliver an innovative solution, it's important to think ahead. For example, minimize operational burdens early in the process by favoring serverless options. In Azure, serverless application options could include [Azure App Service](#) or [containers](#).

In parallel, Azure provides serverless transaction data options that also reduce overhead. The [Azure product catalog](#) provides database options that host data without the need for a full data platform.

## Next steps

Depending on the hypothesis and solution, the principles in this article can aid in designing applications that meet MVP definitions and engage users. Up next are the principles for [empowering adoption](#), which offer ways to get the application and data into the hands of customers more quickly and efficiently.

[Empower adoption](#)

# Empower adoption with digital invention

11/9/2020 • 8 minutes to read • [Edit Online](#)

The ultimate test of innovation is customer reaction to your invention. Did the hypothesis prove true? Do customers use the solution? Does it scale to meet the needs of the desired percentage of users? Most importantly, do they keep coming back? None of these questions can be asked until the minimum viable product (MVP) solution has been deployed. In this article, we'll focus on the discipline of empowering adoption.

## Reduce friction that affects adoption

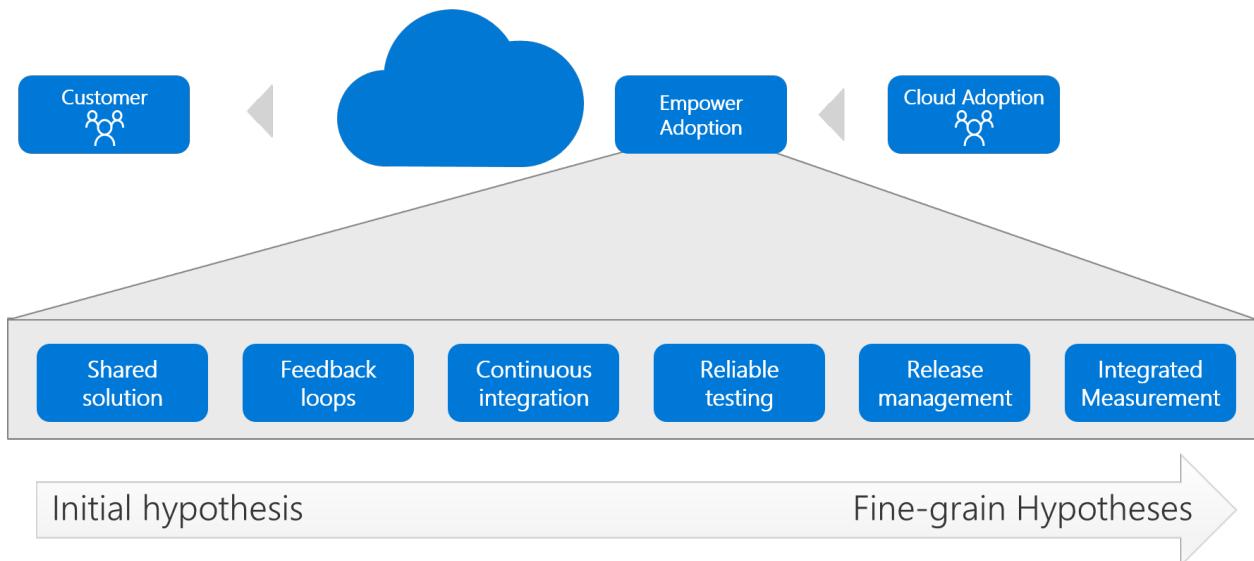
A few key friction points to adoption can be minimized through a combination of technology and processes. For readers with knowledge of continuous integration (CI) and continuous deployment (CD) or DevOps processes, the following will be familiar. This article establishes a starting point for cloud adoption teams that fuels innovation and feedback loops. In the future, this starting point might foster more robust CI/CD or DevOps approaches as the products and teams mature.

As described in [Measure for customer impact](#), positive validation of any hypothesis requires iteration and determination. You'll experience far more failures than wins during any innovation cycle. This is expected. However, when a customer need, hypothesis, and solution align at scale, the world changes quickly. This article aims to minimize [technical spikes](#) that slow innovation but still make sure you keep a few solid best practices in place. Doing so will help the team design for future success while delivering on current customer needs.

## Empower adoption: The maturity model

The primary objective of the [Innovate methodology](#) is to build customer partnerships and accelerate feedback loops, which will lead to market innovations. The following image and sections describe initial implementations that support this methodology.

Empower adoption incrementally, as hypotheses mature



- **Shared solution:** Establish a centralized repository for all aspects of the solution.
- **Feedback loops:** Make sure that feedback loops can be managed consistently through iterations.
- **Continuous integration:** Regularly build and consolidate the solution.
- **Reliable testing:** Validate solution quality and expected changes to ensure the reliability of your testing metrics.
- **Solution deployment:** Deploy solutions so that the team can quickly share changes with customers.

- **Integrated measurement:** Add learning metrics to the feedback loop for clear analysis by the full team.

To minimize technical spikes, assume that maturity will initially be low across each of these principles. But definitely plan ahead by aligning to tools and processes that can scale as hypotheses become more fine-grained. In Azure, the [GitHub](#) and [Azure DevOps](#) allow small teams to get started with little friction. These teams might grow to include thousands of developers who collaborate on scale solutions and test hundreds of customer hypotheses. The remainder of this article illustrates the "plan big, start small" approach to empowering adoption across each of these principles.

## Shared solution

As described in [Measure for customer impact](#), positive validation of any hypothesis requires iteration and determination. You'll experience far more failures than wins during any innovation cycle. This is expected. However, when a customer need, hypothesis, and solution align at scale, the world changes quickly.

When you're scaling innovation, there's no more valuable tool than a shared code base for the solution. Unfortunately, there's no reliable way of predicting which iteration or which MVP will yield the winning combination. That's why it's never too early to establish a shared code base or repository. This is the one [technical spike](#) that should never be delayed. As the team iterates through various MVP solutions, a shared repo enables easy collaboration and accelerated development. When changes to the solution drag down learning metrics, version control lets you roll back to an earlier, more effective version of the solution.

The most widely adopted tool for managing code repositories is [GitHub](#), which lets you create a shared code repository in just a few steps. Additionally, the [Azure Repos](#) feature of Azure DevOps can be used to create a [Git](#) or [TFVC](#) repository.

## Feedback loops

Making the customer part of the solution is the key to building customer partnerships during innovation cycles. That's accomplished, in part, by [measuring customer impact](#). It requires conversations and direct testing with the customer. Both generate feedback that must be managed effectively.

Every point of feedback is a potential solution to the customer need. More importantly, every bit of direct customer feedback represents an opportunity to improve the partnership. If feedback makes it into an MVP solution, celebrate that with the customer. Even if some feedback isn't actionable, simply being transparent with the decision to deprioritize the feedback demonstrates a [growth mindset](#) and a focus on [continuous learning](#).

[Azure DevOps](#) includes ways to [request, provide, and manage feedback](#). Each of these tools centralizes feedback so that the team can take action and provide follow-up in service of a transparent feedback loop.

## Continuous integration

As adoptions scale and a hypothesis gets closer to true innovation at scale, the number of smaller hypotheses to be tested tends to grow rapidly. For accurate feedback loops and smooth adoption processes, it's important that each of those hypotheses is integrated and supportive of the primary hypothesis behind the innovation. This means that you also have to move quickly to innovate and grow, which requires multiple developers for testing variations of the core hypothesis. For later stage development efforts, you might even need multiple teams of developers, each building toward a shared solution. Continuous integration is the first step toward management of all the moving parts.

In continuous integration, code changes are frequently merged into the main branch. Automated build and test processes make sure that code in the main branch is always production quality. This ensures that developers are working together to develop shared solutions that provide accurate and reliable feedback loops.

Azure DevOps and [Azure Pipelines](#) provide continuous integration capabilities with just a few steps in GitHub or a

variety of other repositories. Learn more about [continuous integration](#), or for more information, check out the [hands-on lab](#). Solution architectures are available that can accelerate creation of your [CI/CD pipelines via Azure DevOps](#).

## Reliable testing

Defects in any solution can create false positives or false negatives. Unexpected errors can easily lead to misinterpretation of user adoption metrics. They can also generate negative feedback from customers that doesn't accurately represent the test of your hypothesis.

During early iterations of an MVP solution, defects are expected; early adopters might even find them endearing. In early releases, acceptance testing is typically nonexistent. However, one aspect of building with empathy concerns the validation of the need and hypothesis. Both can be completed through unit tests at a code level and manual acceptance tests before deployment. Together, these provide some means of reliability in testing. You should strive to automate a well-defined series of build, unit, and acceptance tests. These will ensure reliable metrics related to more granular tweaks to the hypothesis and the resulting solution.

The [Azure Test Plans](#) feature provides tooling to develop and operate test plans during manual or automated test execution.

## Solution deployment

Perhaps the most meaningful aspect of empowering adoption concerns your ability to control the release of a solution to customers. By providing a self-service or automated pipeline for releasing a solution to customers, you'll accelerate the feedback loop. By allowing customers to quickly interact with changes in the solution, you invite them into the process. This approach also triggers quicker testing of hypotheses, thereby reducing assumptions and potential rework.

There are several methods for solution deployment. The following represent the three most common:

- **Continuous deployment** is the most advanced method, as it automatically deploys code changes into production. For mature teams that are testing mature hypotheses, continuous deployment can be extremely valuable.
- During early stages of development, **continuous delivery** might be more appropriate. In continuous delivery, any code changes are automatically deployed to a production-like environment. Developers, business decision-makers, and others on the team can use this environment to verify that their work is production-ready. You can also use this method to test a hypothesis with customers without affecting ongoing business activities.
- **Manual deployment** is the least sophisticated approach to release management. As the name suggests, someone on the team manually deploys the most recent code changes. This approach is error prone, unreliable, and considered an antipattern by most seasoned engineers.

During the first iteration of an MVP solution, manual deployment is common, despite the preceding assessment. When the solution is extremely fluid and customer feedback is unknown, there's a significant risk in resetting the entire solution (or even the core hypothesis). Here's the general rule for manual deployment: no customer proof, no deployment automation.

Investing early can lead to lost time. More importantly, it can create dependencies on the release pipeline that make the team more resistant to an early pivot. After the first few iterations or when customer feedback suggests potential success, a more advanced model of deployment should be quickly adopted.

At any stage of hypothesis validation, Azure DevOps and [Azure Pipelines](#) provide continuous delivery and continuous deployment capabilities. Learn more about [continuous delivery](#), or check out the [hands-on lab](#). Solution architecture can also accelerate creation of your [CI/CD pipelines through Azure DevOps](#).

## Integrated measurements

When you [measure for customer impact](#), it's important to understand how customers react to changes in the solution. This data, known as *telemetry*, provides insights into the actions a user (or cohort of users) took when working with the solution. From this data, it's easy to get a quantitative validation of the hypothesis. Those metrics can then be used to adjust the solution and generate more fine-grained hypotheses. Those subtler changes help mature the initial solution in subsequent iterations, ultimately driving to repeat adoption at scale.

In Azure, [Azure Monitor](#) provides the tools and interface to collect and review data from customer experiences. You can apply those observations and insights to refine the backlog by using [Azure Boards](#).

## Next steps

After you've gained an understanding of the tools and processes needed to empower adoption, it's time to examine a more advanced innovation discipline: [interact with devices](#). This discipline can help reduce the barriers between physical and digital experiences, making your solution even easier to adopt.

[Interact with devices](#)

# Ambient experiences: Interact with devices

11/9/2020 • 8 minutes to read • [Edit Online](#)

In [Build with customer empathy](#), we discussed the three tests of true innovation: solve a customer need, keep the customer coming back, and scale across a base of customer cohorts. Each test of your hypothesis requires effort and iterations on the approach to adoption. This article offers insights on some advanced approaches to reduce that effort through *ambient experiences*. By interacting with devices, instead of an application, the customer may be more likely to turn to your solution first.

## Ambient experiences

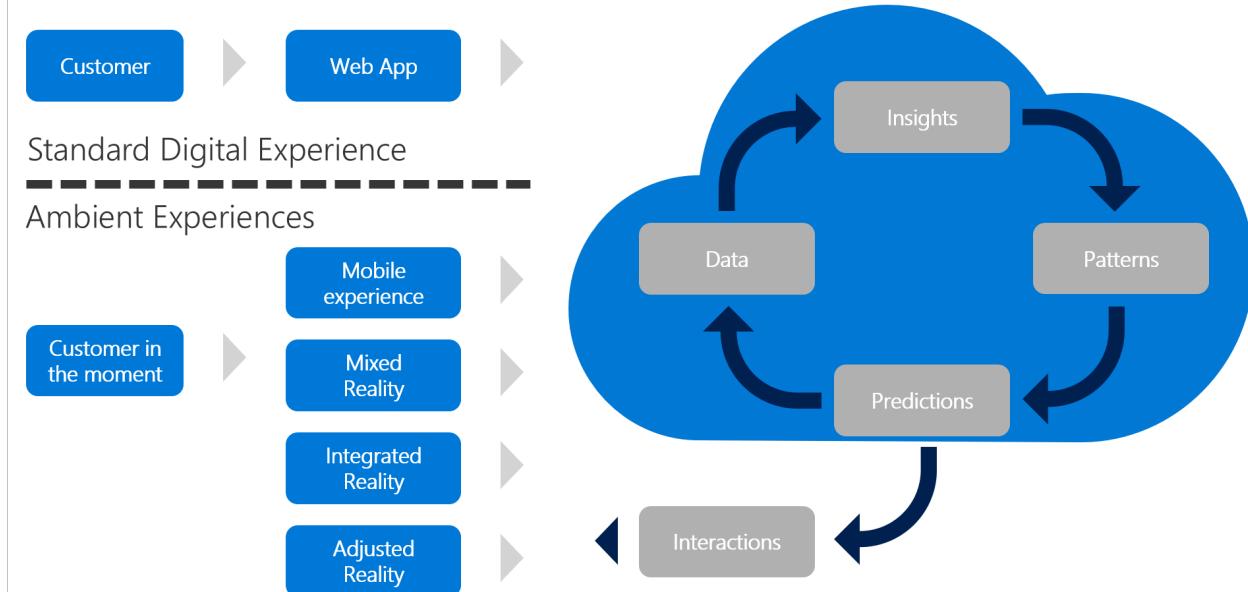
An ambient experience is a digital experience that relates to the immediate surroundings. A solution that features ambient experiences strives to meet the customer in their moment of need. When possible, the solution meets the customer need without leaving the flow of activity that triggered it.

Life in the digital economy is full of distractions. We're all bombarded with social, email, web, visual, and verbal messaging, each of which is a risk of distraction. This risk increases with every second that elapses between the customer's point of need and the moment they encounter a solution. Countless customers are lost in that brief time gap. To foster an increase in repeat adoption, you have to reduce the number of distractions by reducing the time to solution.

## Interact with devices

A standard web experience is the most common application development technique used to meet a customer's needs. This approach assumes that the customer is in front of their computer. If your customer consistently meets their point of need while in front of their laptop, build a web application. That application will provide an ambient experience for that customer in that scenario. However, we know that this scenario is less and less likely in our current era.

### Interacting through devices & ambient experiences



Ambient experiences typically require more than a web application these days. Through [measurement](#) and [learning with the customer](#), the behavior that triggers the customer's need can be observed, tracked, and used to build a more ambient experience. The following list summarizes a few approaches to integration of ambient

solutions into your hypotheses, with more details about each in the following paragraphs.

- **Mobile experience:** As with laptops, mobile apps are ubiquitous in customer environments. In some situations, this might provide a sufficient level of interactivity to make a solution ambient.
- **Mixed reality:** Sometimes a customer's typical surroundings must be altered to make an interaction ambient. This factor creates something of a false reality in which the customer interacts with the solution and has a need met. In this case, the solution is ambient within the false reality.
- **Integrated reality:** Moving closer to true ambience, integrated reality solutions focus on the use of a device that exists within the customer's reality to integrate the solution into their natural behaviors. A Virtual Assistant is a great example of integrating reality into the surrounding environment. A less well-known option concerns Internet of Things (IoT) technologies, which integrate devices that already exist in the customer's surroundings.
- **Adjusted reality:** When any of these ambient solutions use predictive analysis in the cloud to define and provide an interaction with the customer through the natural surroundings, the solution has adjusted reality.

Understanding the customer need and measuring customer impact both help you determine whether a device interaction or ambient experience are necessary to validate your hypothesis. With each of those data points, the following sections will help you find the best solution.

## Mobile experience

In the first stage of ambient experience, the user moves away from the computer. Today's consumers and business professionals move fluidly between mobile and PC devices. Each of the platforms or devices used by your customer creates a new potential experience. Adding a mobile experience that extends the primary solution is the fastest way to improve integration into the customer's immediate surroundings. While a mobile device is far from ambient, it might edge closer to the customer's point of need.

When customers are mobile and change locations frequently, that may represent the most relevant form of ambient experience for a particular solution. Over the past decade, innovation has frequently been triggered by the integration of existing solutions with a mobile experience.

Azure App Service is a great example of this approach. During early iterations, the [web app feature of Azure App Service](#) can be used to test the hypothesis. As the hypotheses become more complex, the [mobile app feature of Azure App Service](#) can extend the web app to run in a variety of mobile platforms.

## Mixed reality

Mixed reality solutions represent the next level of maturity for ambient experiences. This approach augments or replicates the customer's surroundings; it creates an extension of reality for the customer to operate within.

### IMPORTANT

If a VR device is required and it's not already part of a customer's immediate surroundings or natural behaviors, augmented or virtual reality is more of an alternative experience and less of an ambient experience.

Mixed reality experiences are increasingly common among remote workforces. Their use is growing even faster in industries that require collaboration or specialty skills that aren't readily available in the local market. Situations that require centralized implementation support of a complex product for a remote labor force are particularly fertile ground for augmented reality. In these scenarios, the central support team and remote employees might use augmented reality to work on, troubleshoot, and install the product.

For example, consider the case of spatial anchors. Spatial anchors allow you to create mixed reality experiences with objects that persist their respective locations across devices over time. Through spatial anchors, a specific behavior can be captured, recorded, and persisted, thereby providing an ambient experience the next time the user operates within that augmented environment. [Azure Spatial Anchors](#) is a service that moves this logic to the cloud,

allowing experiences to be shared across devices and even across solutions.

## Integrated reality

Beyond mobile reality or even mixed reality lies integrated reality. Integrated reality aims to remove the digital experience entirely. All around us are devices with compute and connectivity capabilities. These devices can be used to collect data from the immediate surroundings without the customer having to ever touch a phone, laptop, or virtual reality (VR) device.

This experience is ideal when some form of device is consistently within the same surroundings in which the customer need occurs. Common scenarios include factory floors, elevators, and even your car. These types of large devices already contain compute power. You can also use data from the device itself to detect customer behaviors and send those behaviors to the cloud. This automatic capture of customer behavior data dramatically reduces the need for a customer to input data. Additionally, the web, mobile, or VR experience can function as a feedback loop to share what's been learned from the integrated reality solution.

Examples of integrated reality in Azure could include:

- [Azure Internet of Things \(IoT\) solutions](#): A collection of services in Azure that aid in managing devices and the flow of data from those devices into the cloud and back out to end users.
- [Azure Sphere](#): A combination of hardware and software that provides an intrinsically secure way to enable an existing device to securely transmit data between the device and Azure IoT solutions.
- [Azure Kinect DK](#), AI sensors with advanced computer vision and speech models. These sensors can collect visual and audio data from the immediate surroundings and feed those inputs into your solution.

You can use all three of these tools to collect data from the natural surroundings and at the point of customer need. From there, your solution can respond to those data inputs to solve the need, sometimes before the customer is even aware that a trigger for that need has occurred.

## Adjusted reality

The highest form of ambient experience is adjusted reality, often referred to as *ambient intelligence*. Adjusted reality is an approach to using information from your solution to change the customer's reality without requiring them to interact directly with an application. In this approach, the application you initially built to prove your hypothesis might no longer be relevant at all. Instead, devices in the environment help modulate the inputs and outputs to meet customer needs.

Virtual assistants and smart speakers offer great examples of adjusted reality. Alone, a smart speaker is an example of simple integrated reality. But add a smart light and motion sensor to a smart speaker solution and it's easy to create a basic solution that turns on the lights when you enter a room.

Factory floors around the world provide additional examples of adjusted reality. During early stages of integrated reality, sensors on devices detected conditions like overheating, and then alerted a human being through an application. In adjusted reality, the customer might still be involved, but the feedback loop is tighter. On an adjusted reality factory floor, one device might detect overheating in a vital machine somewhere along the assembly line. Somewhere else on the floor, a second device then slows production slightly to allow the machine to cool and then resume full pace when the condition is resolved. In this situation, the customer is a second-hand participant. The customer uses your application to set the rules and understand how those rules have affected production, but they're not necessary to the feedback loop.

The Azure services described in [Azure Internet of Things \(IoT\) solutions](#), [Azure Sphere](#), and [Azure Kinect DK](#) can all be components of an adjusted reality solution. Your original application and business logic would then serve as the intermediary between the environmental input and the change that should be made in the physical environment.

A digital twin is another example of adjusted reality. This term refers to a digital representation of a physical

device, presented through computer, mobile, or mixed-reality formats. Unlike less sophisticated 3D models, a digital twin reflects data collected from an actual device in the physical environment. This solution allows the user to interact with the digital representation in ways that could never be done in the real world. In this approach, physical devices adjust a mixed reality environment. However, the solution still gathers data from an integrated reality solution and uses that data to shape the reality of the customer's current surroundings.

In Azure, digital twins are created and accessed through a service called [Azure Digital Twins](#).

## Next steps

Now that you have a deeper understanding of device interactions and the ambient experience that's right for your solution, you're ready to explore the final discipline of innovation, [predict and influence](#).

[Predict and influence](#)

# Predict and influence

11/9/2020 • 5 minutes to read • [Edit Online](#)

There are two classes of applications in the digital economy: *historical* and *predictive*. Many customer needs can be met solely by using historical data, including nearly real-time data. Most solutions focus primarily on aggregating data in the moment. They then process and share that data back to the customer in the form of a digital or ambient experience.

As predictive modeling becomes more cost-effective and readily available, customers demand forward-thinking experiences that lead to better decisions and actions. However, that demand doesn't always suggest a predictive solution. In most cases, a historical view can provide enough data to empower the customer to make a decision on their own.

Unfortunately, customers often take a myopic view that leads to decisions based on their immediate surroundings and sphere of influence. As options and decisions grow in number and impact, that myopic view may not serve the customer's needs. At the same time, as a hypothesis is proven at scale, the company providing the solution can see across thousands or millions of customer decisions. This big-picture approach makes it possible to see broad patterns and the impacts of those patterns. Predictive capability is a wise investment when an understanding of those patterns is necessary to make decisions that best serve the customer.

## Examples of predictions and influence

A variety of applications and ambient experiences use data to make predictions:

- **E-commerce:** Based on what other similar consumers have purchased, an e-commerce website suggests products that may be worth adding to your cart.
- **Adjusted reality:** IoT offers more advanced instances of predictive functionality. For example, a device on an assembly line detects a rise in a machine's temperature. A cloud-based predictive model determines how to respond. Based on that prediction, another device slows down the assembly line until the machine can cool.
- **Consumer products:** Cell phones, smart homes, even your car, all use predictive capabilities, which they analyze to suggest user behavior based on factors like location or time of day. When a prediction and the initial hypothesis are aligned, the prediction leads to action. At a very mature stage, this alignment can make products like a self-driving car a reality.

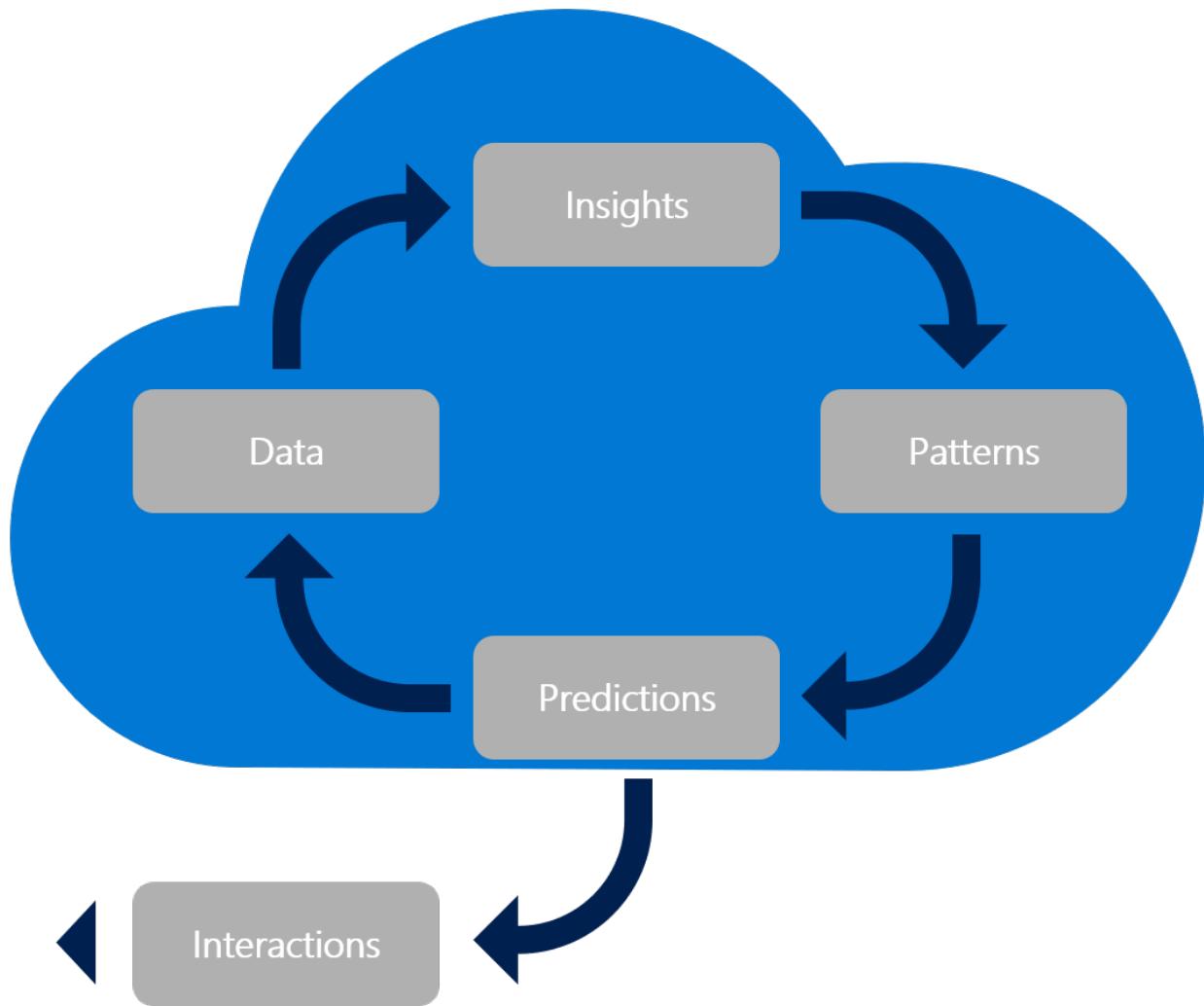
## Develop predictive capabilities

Solutions that consistently provide accurate predictive capabilities commonly include five core characteristics:

- Data
- Insights
- Patterns
- Predictions
- Interactions

Each aspect is required to develop predictive capabilities. Like all great innovations, the development of predictive capabilities requires a [commitment to iteration](#). In each iteration, one or more of the following characteristics is matured to validate increasingly complex customer hypotheses.

# Predict & Influence



## Caution

If the customer hypothesis developed in [Build with customer empathy](#) includes predictive capabilities, the principles described there might well apply. However, predictive capabilities require significant investment of time and energy. When predictive capabilities are [technical spikes](#), as opposed to a source of real customer value, we suggest that you delay predictions until the customer hypotheses have been validated at scale.

## Data

Data is the most elemental of the characteristics mentioned earlier. Each of the disciplines for developing digital inventions generates data. That data, of course, contributes to the development of predictions. For more guidance on ways to get data into a predictive solution, see [Democratizing data](#) and [interacting with devices](#).

A variety of data sources can be used to deliver predictive capabilities:

## Insights

Subject matter experts use data about customer needs and behaviors to develop basic business insights from a study of raw data. Those insights can pinpoint occurrences of the desired customer behaviors (or, alternatively, undesirable results). During iterations on the predictions, these insights can aid in identifying potential correlations that could ultimately generate positive outcomes. For guidance on enabling subject matter experts to develop insights, see [Democratizing data](#).

## Patterns

People have always tried to detect patterns in large volumes of data. Computers were designed for that purpose. Machine learning accelerates that quest by detecting precisely such patterns, a skill that comprises the machine learning model. Those patterns are then applied through machine learning algorithms to predict outcomes when a new set of data is entered into the algorithms.

Using insights as a starting point, machine learning develops and applies predictive models to capitalize on the patterns in data. Through multiple iterations of training, testing, and adoption, those models and algorithms can accurately predict future outcomes.

[Azure Machine Learning](#) is the cloud-native service in Azure for building and training models based on your data. This tool also includes a [workflow for accelerating the development of machine learning algorithms](#). This workflow can be used to develop algorithms through a visual interface or Python.

For more robust machine learning models, [ML Services in Azure HDInsight](#) provides a machine learning platform built on Apache Hadoop clusters. This approach enables more granular control of the underlying clusters, storage, and compute nodes. Azure HDInsight also offers more advanced integration through tools like ScaleR and SparkR to create predictions based on integrated and ingested data, even working with data from a stream. The [flight delay prediction solution](#) demonstrates each of these advanced capabilities when used to predict flight delays based on weather conditions. The HDInsight solution also allows for enterprise controls, such as data security, network access, and performance monitoring to operationalize patterns.

## Predictions

After a pattern is built and trained, you can apply it through APIs, which can make predictions during the delivery of a digital experience. Most of these APIs are built from a well-trained model based on a pattern in your data. As more customers deploy everyday workloads to the cloud, the prediction APIs used by cloud providers lead to ever-faster adoption.

[Azure Cognitive Services](#) is an example of a predictive API built by a cloud vendor. This service includes predictive APIs for content moderation, anomaly detection, and suggestions to personalize content. These APIs are ready to use and are based on well-known content patterns, which Microsoft has used to train models. Each of those APIs makes predictions based on the data you feed into the API.

[Azure Machine Learning](#) lets you deploy custom-built algorithms, which you can create and train based solely on your own data. Learn more about deploying predictions with [Azure Machine Learning](#).

[Set up HDInsight clusters](#) discusses the processes for exposing predictions developed for ML Services on Azure HDInsight.

## Interactions

After a prediction is made available through an API, you can use it to influence customer behavior. That influence takes the form of interactions. An interaction with a machine learning algorithm happens within your other digital or ambient experiences. As data is collected through the application or experience, it's run through the machine learning algorithms. When the algorithm predicts an outcome, that prediction can be shared back with the customer through the existing experience.

Learn more about how to create an ambient experience through an [adjusted reality solution](#).

## Next steps

Having acquainted yourself with [disciplines of invention](#) and the [Innovate methodology](#), you're now ready to learn how to [build with customer empathy](#).

[Build with empathy](#)

# Governance in the Microsoft Cloud Adoption Framework for Azure

11/9/2020 • 3 minutes to read • [Edit Online](#)

The cloud creates new paradigms for the technologies that support the business. These new paradigms also change how those technologies are adopted, managed, and governed. When entire datacenters can be virtually torn down and rebuilt with one line of code executed by an unattended process, we have to rethink traditional approaches. This is especially true for governance.

Cloud governance is an iterative process. For organizations with existing policies that govern on-premises IT environments, cloud governance should complement those policies. The level of corporate policy integration between on-premises and the cloud varies depending on cloud governance maturity and a digital estate in the cloud. As the cloud estate changes over time, so do cloud governance processes and policies. The following exercises help you start building your initial governance foundation.

1. **Methodology:** Establish a basic understanding of the methodology that drives cloud governance in the Cloud Adoption Framework to begin thinking through the end state solution.
2. **Benchmark:** Assess your current state and future state to establish a vision for applying the framework.
3. **Initial governance foundation:** Begin your governance journey with a small, easily implemented set of governance tools. This initial governance foundation is called a minimum viable product (MVP).
4. **Improve the initial governance foundation:** Throughout implementation of the cloud adoption plan, iteratively add governance controls to address tangible risks as you progress toward the end state.

## Objective of this content

The guidance in this section of the Cloud Adoption Framework serves two purposes:

- Provide examples of actionable governance guides that represent common experiences often encountered by customers. Each example encapsulates business risks, corporate policies for risk mitigation, and design guidance for implementing technical solutions. By necessity, the design guidance is specific to Azure. All other content in these guides could be applied in a cloud-agnostic or multicloud approach.
- Help you create personalized governance solutions that meet a variety of business needs. These needs include the governance of multiple public clouds through detailed guidance on the development of corporate policies, processes, and tooling.

This content is intended for use by the cloud governance team. It's also relevant to cloud architects who need to develop a strong foundation in cloud governance.

## Intended audience

The content in the Cloud Adoption Framework affects the business, technology, and culture of enterprises. This section of the Cloud Adoption Framework interacts heavily with IT security, IT governance, finance, line-of-business leaders, networking, identity, and cloud adoption teams. Various dependencies on these personnel require a facilitative approach by the cloud architects using this guidance. Facilitation with these teams might be a one-time effort. In some cases, interactions with these other personnel will be ongoing.

The cloud architect serves as the thought leader and facilitator to bring these audiences together. The content in this collection of guides is designed to help the cloud architect facilitate the right conversation, with the right audience, to drive necessary decisions. Business transformation that's empowered by the

cloud depends on the cloud architect to help guide decisions throughout the business and IT.

**Cloud architect specialization in this section:** Each section of the Cloud Adoption Framework represents a different specialization or variant of the cloud architect role. This section of the Cloud Adoption Framework is designed for cloud architects with a passion for mitigating or reducing technical risks. Some cloud providers refer to these specialists as *cloud custodians*, but we prefer *cloud guardians* or, collectively, the *cloud governance team*. The actionable governance guides show how the composition and role of the cloud governance team might change over time.

## Use this guide

Reading the Govern methodology content end-to-end will help you develop a robust cloud governance strategy in parallel with cloud implementation. The guidance walks you through the theory and implementation of this strategy.

For a crash course on the theory and quick access to Azure implementation, get started with the [governance guides overview](#). Using this guidance, you can start small and iteratively improve your governance needs in parallel with cloud adoption efforts.

# Govern methodology for the cloud

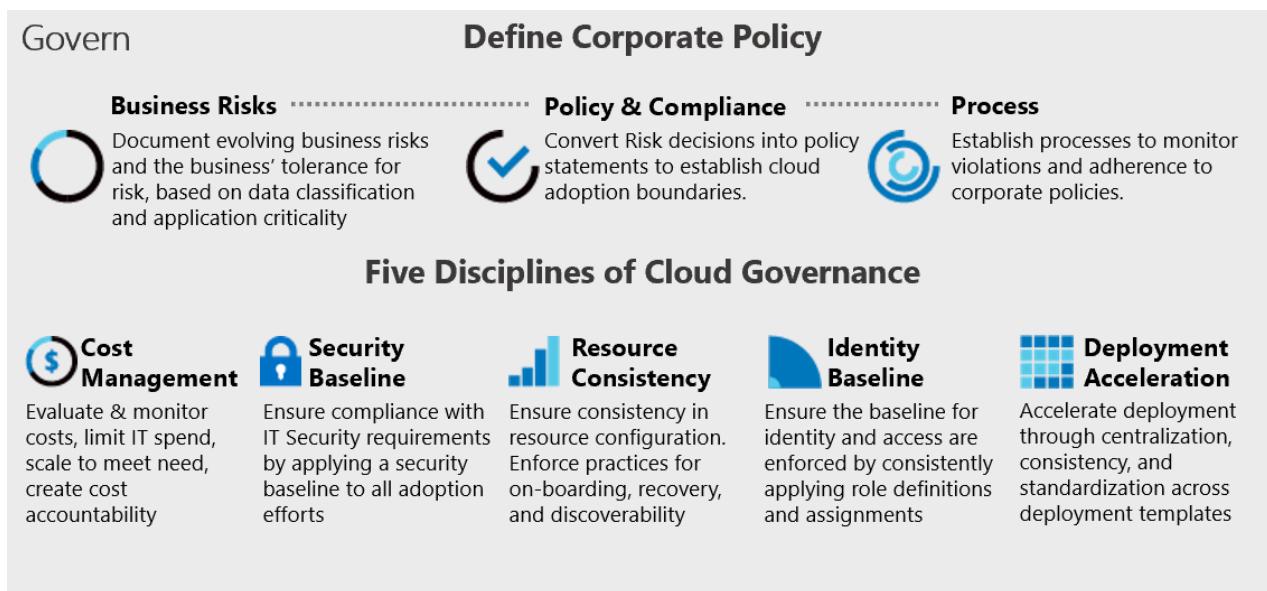
11/9/2020 • 3 minutes to read • [Edit Online](#)

Adopting the cloud is a journey, not a destination. Along the way, there are clear milestones and tangible business benefits. The final state of cloud adoption is unknown when a company begins the journey. Cloud governance creates guardrails that keep the company on a safe path throughout the journey.

The Cloud Adoption Framework provides governance guides that describe the experiences of fictional companies that are based on the experiences of real customers. Each guide follows the customer through the governance aspects of their cloud adoption.

## Envision an end state

A journey without a target destination is just wandering. It's important to establish a rough vision of the end state before taking the first step. The following infographic provides a frame of reference for the end state. It's not your starting point, but it shows your potential destination.



The Cloud Adoption Framework governance model identifies key areas of importance during the journey. Each area relates to different types of risks the company must address as it adopts more cloud services. Within this framework, the governance guide identifies required actions for the cloud governance team. Along the way, each principle of the Cloud Adoption Framework governance model is described further. Broadly, these include:

**Corporate policies:** Corporate policies drive cloud governance. The governance guide focuses on specific aspects of corporate policy:

- **Business risks:** Identifying and understanding corporate risks.
- **Policy and compliance:** Converting risks into policy statements that support any compliance requirements.
- **Processes:** Ensuring adherence to the stated policies.

**Five Disciplines of Cloud Governance:** These disciplines support the corporate policies. Each discipline protects the company from potential pitfalls:

- Cost Management discipline
- Security Baseline discipline
- Resource Consistency discipline

- Identity Baseline discipline
- Deployment Acceleration discipline

Essentially, corporate policies serve as the early warning system to detect potential problems. The disciplines help the company manage risks and create guardrails.

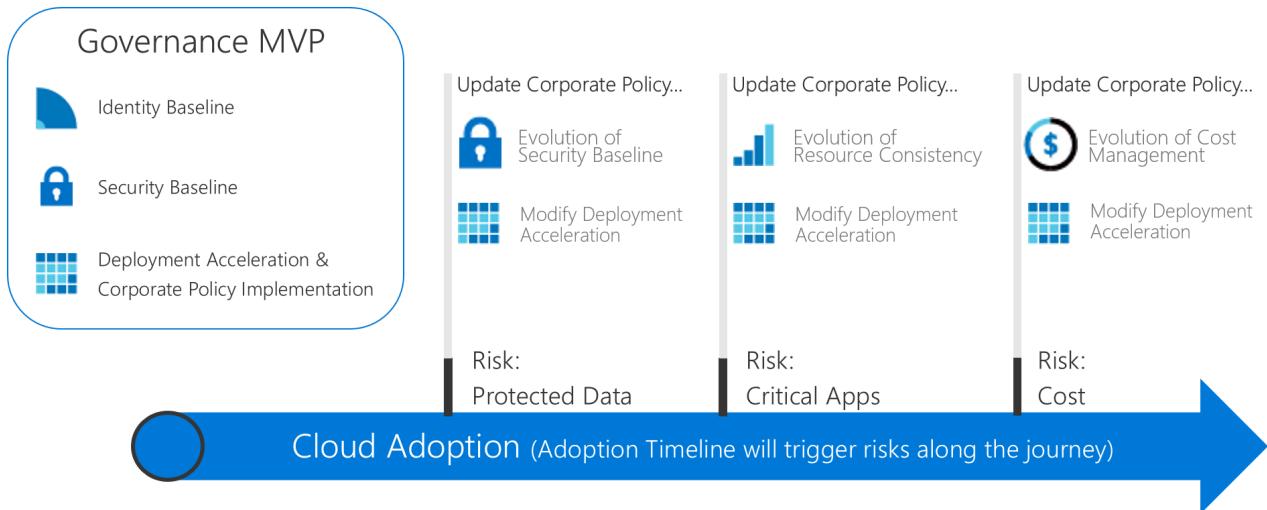
## Grow to the end state

Because governance requirements will change throughout the cloud adoption journey, a different approach to governance is required. Companies can no longer wait for a small team to build guardrails and roadmaps on every highway **before taking the first step**. Business results are expected more quickly and smoothly. IT governance must also move quickly and keep pace with business demands to stay relevant during cloud adoption and avoid "shadow IT."

An *incremental governance* approach empowers these traits. Incremental governance relies on a small set of corporate policies, processes, and tools to establish a foundation for adoption and governance. That foundation is called a *minimum viable product (MVP)*. An MVP allows the governance team to quickly incorporate governance into implementations throughout the adoption lifecycle. An MVP can be established at any point during the cloud adoption process. It's a good practice to adopt an MVP as early as possible.

The ability to respond rapidly to changing risks empowers the cloud governance team to engage in new ways. The cloud governance team can join the cloud strategy team as scouts, moving ahead of the cloud adoption teams, plotting routes, and quickly establishing guardrails to manage risks associated with the adoption plans. These just-in-time governance layers are known as *governance iterations*. With this approach, governance strategy grows one step ahead of the cloud adoption teams.

The following diagram shows a simple governance MVP and three governance iterations. During the iterations, additional corporate policies are defined to remediate new risks. The Deployment Acceleration discipline then applies those changes across each deployment.



### NOTE

Governance is not a replacement for key functions such as security, networking, identity, finance, DevOps, or operations. Along the way, there will be interactions with and dependencies on members from each function. Those members should be included on the cloud governance team to accelerate decisions and actions.

## Next steps

Learn to use the Cloud Adoption Framework governance benchmark tool to assess your transformation journey and help you identify gaps in your organization across six key domains as defined in the framework.

Assess your transformation journey

# Assess your transformation journey

5/19/2020 • 2 minutes to read • [Edit Online](#)

The Cloud Adoption Framework provides a [governance benchmark tool](#) to help you identify gaps in your organization across six key domains as defined in the framework.

## Governance benchmark tool

Receive a personalized report that outlines the difference between your current state and business priorities, along with tailored resources to help you get started. Assess your current state and future state to establish a vision for applying the framework.

[Use the governance benchmark tool](#)

## Next steps

Begin your governance journey with a small, easily implemented set of governance tools. This initial governance foundation is called a minimum viable product (MVP).

[Establish an initial governance foundation](#)

# Establish an initial cloud governance foundation

11/9/2020 • 2 minutes to read • [Edit Online](#)

Establishing cloud governance is a broad iterative effort. It is challenging to strike an effective balance between speed and control, especially during execution of early methodologies within the cloud adoption. The governance guidance in the Cloud Adoption Framework helps provide that balance via an agile approach to adoption.

This article provides two options for establishing an initial foundation for governance. Either option ensures that governance constraints can be scaled and expanded as the adoption plan is implemented and requirements become more clearly defined. By default, the initial foundation assumes an isolate-and-control position. It also focuses more on resource organization than on resource governance. This lightweight starting point is called a *minimum viable product (MVP)* for governance. The objective of the MVP is reducing barriers to establishing an initial governance position, and then enabling rapid maturation of the solution to address a variety of tangible risks.

## Already using the Cloud Adoption Framework

If you have been following along with the Cloud Adoption Framework, you may have already deployed a governance MVP. Governance is a core aspect of any operating model. It is present in every methodology of the cloud adoption lifecycle. As such, the [Cloud Adoption Framework](#) provides guidance that injects governance into activities related to the implementation of your [cloud adoption plan](#). One example of this governance integration is using blueprints to deploy one or more landing zones present in the [Ready methodology](#) guidance. Another example is guidance for [scaling out subscriptions](#). If you have followed either of those recommendations, then the following MVP sections are simply a review of your existing deployment decisions. After a quick review, jump ahead to [mature the initial governance solution and apply best-practice controls](#).

## Establish an initial governance foundation

The following are two different examples of initial governance foundations (also called governance MVPs) to apply a sound foundation for governance to new or existing deployments. Choose the MVP that best aligns with your business needs to get started:

- [Standard governance guide](#): A guide for most organizations based on the recommended initial two-subscription model, designed for deployments in multiple regions but not spanning public and sovereign/government clouds.
- [Governance guide for complex enterprises](#): A guide for enterprises that are managed by multiple independent IT business units or span public and sovereign/government clouds.

## Next steps

Once a governance foundation is in place, apply suitable recommendations to improve the solution and protect against tangible risks.

[Improve the initial governance foundation](#)

# Improve your initial cloud governance foundation

11/9/2020 • 2 minutes to read • [Edit Online](#)

This article assumes that you have established an [initial cloud governance foundation](#). As your cloud adoption plan is implemented, tangible risks will emerge from the proposed approaches by which teams want to adopt the cloud. As these risks surface in release planning conversations, use the following grid to quickly identify a few best practices for getting ahead of the adoption plan to prevent risks from becoming real threats.

## Maturity vectors

At any time, the following best practices can be applied to the initial governance foundation to address the risk or need mentioned in the table below.

### IMPORTANT

Resource organization can affect how these best practices are applied. It is important to start with the recommendations that best align with the initial cloud governance foundation you implemented in the previous step.

RISK/NEED	STANDARD ENTERPRISE	COMPLEX ENTERPRISE
Sensitive data in the cloud	<a href="#">Discipline improvement</a>	<a href="#">Discipline improvement</a>
Mission-critical applications in the cloud	<a href="#">Discipline improvement</a>	<a href="#">Discipline improvement</a>
Cloud cost management	<a href="#">Discipline improvement</a>	<a href="#">Discipline improvement</a>
Multicloud	<a href="#">Discipline improvement</a>	<a href="#">Discipline improvement</a>
Complex/legacy identity management	N/A	<a href="#">Discipline improvement</a>
Multiple layers of governance	N/A	<a href="#">Discipline improvement</a>

## Next steps

In addition to the application of best practices, the Govern methodology of the Cloud Adoption Framework can be customized to fit unique business constraints. After following the applicable recommendations, [evaluate corporate policy to understand additional customization requirements](#).

[Evaluate corporate policy](#)

# Cloud governance guides

11/9/2020 • 5 minutes to read • [Edit Online](#)

The actionable governance guides in this section illustrate the incremental approach of the Cloud Adoption Framework governance model, based on the [Govern methodology](#) previously described. You can establish an agile approach to cloud governance that will grow to meet the needs of any cloud governance scenario.

## Review and adopt cloud governance best practices

To begin your cloud adoption journey, choose one of the following governance guides. Each guide outlines a set of best practices, based on a set of fictional customer experiences. For readers who are new to the incremental approach of the Cloud Adoption Framework governance model, review the high-level introduction to governance theory below before adopting either set of best practices.

- [Standard governance guide](#): A guide for most organizations based on the recommended two-subscription model, designed for deployments in multiple regions but not spanning public and sovereign/government clouds.

### [Standard governance guide](#)

- [Governance guide for complex enterprises](#): A guide for enterprises that are managed by multiple independent IT business units or span public and sovereign/government clouds.

### [Governance guide for complex enterprises](#)

## An incremental approach to cloud governance

### Choose a governance guide

The guides demonstrate how to implement a governance MVP. From there, each guide shows how the cloud governance team can work ahead of the cloud adoption teams as a partner to accelerate adoption efforts. The Cloud Adoption Framework governance model guides the application of governance from foundation through subsequent improvements and evolutions.

To begin a governance journey, choose one of the two options below. The options are based on synthesized customer experiences. The titles are based on the complexity of the enterprise for ease of navigation. Your decision may be more complex. The following tables outline the differences between the two options.

#### **WARNING**

A more robust governance starting point may be required. In such cases, consider the [CAF enterprise-scale landing zone](#). This approach focuses on adoption teams who have a mid-term objective (within 24 months) to host more than 1,000 assets (infrastructure, apps, or data) in the cloud. The CAF enterprise-scale landing zone is the typical choice for complex governance scenarios in large cloud adoption efforts.

#### **NOTE**

It's unlikely that either guide aligns entirely with your situation. Choose whichever guide is closest and use it as a starting point. Throughout the guide, additional information is provided to help you customize decisions to meet specific criteria.

## Business characteristics

CHARACTERISTIC	STANDARD ORGANIZATION	COMPLEX ENTERPRISE
Geography (country or geopolitical region)	Customers or staff reside largely in one geography	Customers or staff reside in multiple geographies or require sovereign clouds.
Business units affected	Business units that share a common IT infrastructure	Multiple business units that do not share a common IT infrastructure.
IT budget	Single IT budget	Budget allocated across business units and currencies.
IT investments	Capital expense-driven investments are planned yearly and usually cover only basic maintenance.	Capital expense-driven investments are planned yearly and often include maintenance and a refresh cycle of three to five years.

## Current state before adopting cloud governance

STATE	STANDARD ENTERPRISE	COMPLEX ENTERPRISE
Datacenter or third-party hosting providers	Fewer than five datacenters	More than five datacenters
Networking	No WAN, or 1 – 2 WAN providers	Complex network or global WAN
Identity	Single forest, single domain.	Complex, multiple forests, multiple domains.

## Desired future state after incremental improvement of cloud governance

STATE	STANDARD ORGANIZATION	COMPLEX ENTERPRISE
Cost Management: cloud accounting	Showback model. Billing is centralized through IT.	Chargeback model. Billing could be distributed through IT procurement.
Security Baseline: protected data	Company financial data and IP. Limited customer data. No third-party compliance requirements.	Multiple collections of customers' financial and personal data. Might need to consider third-party compliance.

## CAF enterprise-scale landing zone

[CAF enterprise-scale landing zone](#) is an approach to making the most of the Azure cloud platform's capabilities while respecting an enterprise's security and governance requirements.

Compared to traditional on-premises environments, Azure allows workload development teams and their business sponsors to take advantage of the increased deployment agility that cloud platforms offer. As your cloud adoption efforts expand to include mission-critical data and workloads, this agility may conflict with corporate security and policy compliance requirements established by your IT teams. This is especially true for large enterprises that have existing sophisticated governance and regulatory requirements.

The CAF enterprise-scale landing zone architecture aims to address these concerns earlier in the adoption lifecycle by architectures, implementations, and guidance to help achieve a balance between cloud adoption team requirements and central IT team requirements during enterprise cloud adoption efforts. Central to this

approach is the concept of a shared service architecture and well-managed landing zones.

CAF enterprise-scale landing zone deploys your own "isolated cloud" within the Azure platform, integrating management processes, regulatory requirements, and security processes required by your governance policies. Within this virtual boundary, CAF enterprise-scale landing zone offers example models for deploying workloads while ensuring consistent compliance and provides basic guidance on implementing an organization's separation of roles and responsibilities in the cloud.

### **CAF enterprise-scale landing zone qualifications**

Although smaller teams may benefit from the architecture and recommendations the CAF enterprise-scale landing zone provides. Our objective is to continue to streamline the CAF enterprise-scale landing zone implementations to make them more friendly for smaller teams. Currently, this approach is designed to guide central IT teams managing large cloud environments.

The [CAF enterprise-scale landing zone](#) approach focuses on adoption teams who have a mid-term objective (within 24 months) to **host more than 1,000 assets (applications, infrastructure, or data assets) in the cloud**.

For organizations that meet the following criteria, you may also want to start with the [CAF enterprise-scale landing zone](#):

- Your enterprise is subject to regulatory compliance requirements that require centralized monitoring and audit capabilities.
- You need to maintain common policy and governance compliance and centralized IT control over core services.
- Your industry depends on a complex platform that requires complex controls and deep domain expertise to govern the platform. This is most common in large enterprises within finance, manufacturing, and oil and gas.
- Your existing IT governance policies require tighter parity with existing features, even during early stage adoption.

## Next steps

Choose one of these guides:

[Standard enterprise governance guide](#)

[Governance guide for complex enterprises](#)

# Standard enterprise governance guide

11/9/2020 • 8 minutes to read • [Edit Online](#)

## Overview of best practices

This governance guide follows the experiences of a fictional company through various stages of governance maturity. It is based on real customer experiences. The best practices are based on the constraints and needs of the fictional company.

As a quick starting point, this overview defines a minimum viable product (MVP) for governance based on best practices. It also provides links to some governance improvements that add further best practices as new business or technical risks emerge.

### WARNING

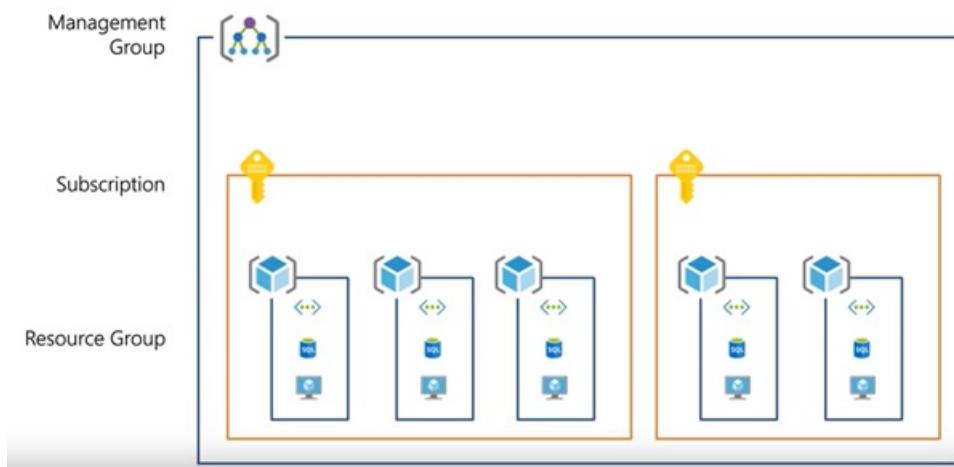
This MVP is a baseline starting point, based on a set of assumptions. Even this minimal set of best practices is based on corporate policies that are driven by unique business risks and risk tolerances. To see whether these assumptions apply to you, read the [longer narrative](#) that follows this article.

## Governance best practices

These best practices serve as a foundation for an organization to quickly and consistently add governance guardrails across your subscriptions.

### Resource organization

The following diagram shows the governance MVP hierarchy for organizing resources.

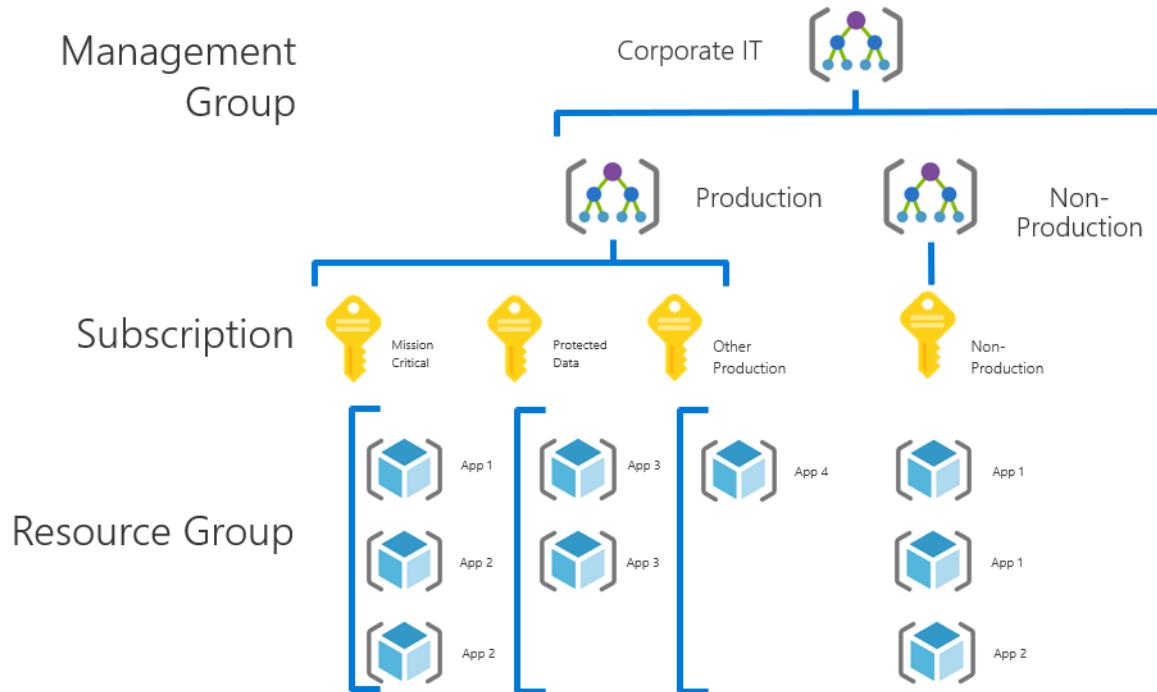


Every application should be deployed in the proper area of the management group, subscription, and resource group hierarchy. During deployment planning, the cloud governance team will create the necessary nodes in the hierarchy to empower the cloud adoption teams.

1. One management group for each type of environment (such as production, development, and test).
2. Two subscriptions, one for production workloads and another for nonproduction workloads.
3. [Consistent nomenclature](#) should be applied at each level of this grouping hierarchy.
4. Resource groups should be deployed in a manner that considers its contents lifecycle: everything that is developed together, is managed together, and retires together goes together. For more information about resource group best practices, see the [resource consistency decision guide](#).
5. [Region selection](#) is incredibly important and must be considered so that networking, monitoring, auditing can

be in place for failover/failback as well as confirmation that [needed SKUs are available in the preferred regions](#).

Here is an example of this pattern in use:



These patterns provide room for growth without complicating the hierarchy unnecessarily.

#### NOTE

In the event of changes to your business requirements, Azure management groups allow you to easily reorganize your management hierarchy and subscription group assignments. However, keep in mind that policy and role assignments applied to a management group are inherited by all subscriptions underneath that group in the hierarchy. If you plan to reassigned subscriptions between management groups, make sure that you are aware of any policy and role assignment changes that may result. See the [Azure management groups documentation](#) for more information.

## Governance of resources

A set of global policies and RBAC roles will provide a baseline level of governance enforcement. To meet the cloud governance team's policy requirements, implementing the governance MVP requires completing the following tasks:

1. Identify the Azure Policy definitions needed to enforce business requirements. This might include using built-in definitions and creating new custom definitions. To keep up with the pace of newly released built-in definitions, there's an [atom feed](#) of all the commits for built-in policies, which you can use for an RSS feed. Alternatively, you can check [AzAdvertiser](#).
2. Create a blueprint definition using these built-in and custom policy and the role assignments required by the governance MVP.
3. Apply policies and configuration globally by assigning the blueprint definition to all subscriptions.

#### Identify policy definitions

Azure provides several built-in policies and role definitions that you can assign to any management group, subscription, or resource group. Many common governance requirements can be handled using built-in definitions. However, it's likely that you will also need to create custom policy definitions to handle your specific requirements.

Custom policy definitions are saved to either a management group or a subscription and are inherited through the management group hierarchy. If a policy definition's save location is a management group, that policy definition is available to assign to any of that group's child management groups or subscriptions.

Since the policies required to support the governance MVP are meant to apply to all current subscriptions, the following business requirements will be implemented using a combination of built-in definitions and custom definitions created in the root management group:

1. Restrict the list of available role assignments to a set of built-in Azure roles authorized by your cloud governance team. This requires a [custom policy definition](#).
2. Require the following tags on all resources: *Department/Billing Unit, Geography, Data Classification, Criticality, SLA, Environment, Application Archetype, Application, and Application Owner*. This can be handled using the [Require specified tag](#) built-in definition.
3. Require that the [Application](#) tag for resources should match the name of the relevant resource group. This can be handled using the "Require tag and its value" built-in definition.

For information on defining custom policies see the [Azure Policy documentation](#). For guidance and examples of custom policies, consult the [Azure Policy samples site](#) and the associated [GitHub repository](#).

#### Assign Azure Policy and RBAC roles using Azure Blueprints

Azure policies can be assigned at the resource group, subscription, and management group level, and can be included in [Azure Blueprints](#) definitions. Although the policy requirements defined in this governance MVP apply to all current subscriptions, it's very likely that future deployments will require exceptions or alternative policies. As a result, assigning policy using management groups, with all child subscriptions inheriting these assignments, may not be flexible enough to support these scenarios.

Azure Blueprints allows consistent assignment of policy and roles, application of Resource Manager templates, and deployment of resource groups across multiple subscriptions. Like policy definitions, blueprint definitions are saved to management groups or subscriptions. The policy definitions are available through inheritance to any children in the management group hierarchy.

The cloud governance team has decided that enforcement of required Azure Policy and RBAC assignments across subscriptions will be implemented through Azure Blueprints and associated artifacts:

1. In the root management group, create a blueprint definition named [governance-baseline](#).
2. Add the following blueprint artifacts to the blueprint definition:
  - a. Policy assignments for the custom Azure Policy definitions defined at the management group root.
  - b. Resource group definitions for any groups required in subscriptions created or governed by the Governance MVP.
  - c. Standard role assignments required in subscriptions created or governed by the Governance MVP.
3. Publish the blueprint definition.
4. Assign the [governance-baseline](#) blueprint definition to all subscriptions.

See the [Azure Blueprints documentation](#) for more information on creating and using blueprint definitions.

#### Secure hybrid VNet

Specific subscriptions often require some level of access to on-premises resources. This is common in migration scenarios or dev scenarios where dependent resources reside in the on-premises datacenter.

Until trust in the cloud environment is fully established it's important to tightly control and monitor any allowed communication between the on-premises environment and cloud workloads, and that the on-premises network is secured against potential unauthorized access from cloud-based resources. To support these scenarios, the governance MVP adds the following best practices:

1. Establish a cloud secure hybrid VNet.

- a. The [VPN reference architecture](#) establishes a pattern and deployment model for creating a VPN Gateway in Azure.
  - b. Validate that on-premises security and traffic management mechanisms treat connected cloud networks as untrusted. Resources and services hosted in the cloud should only have access to authorized on-premises services.
  - c. Validate that the local edge device in the on-premises datacenter is compatible with [Azure VPN Gateway requirements](#) and is configured to access the public internet.
  - d. Note that VPN tunnels should not be considered production ready circuits for anything but the most simple workloads. Anything beyond a few simple workloads requiring on-premises connectivity should use Azure ExpressRoute.
2. In the root management group, create a second blueprint definition named `secure-hybrid-vnet`.
    - a. Add the Resource Manager template for the VPN Gateway as an artifact to the blueprint definition.
    - b. Add the Resource Manager template for the virtual network as an artifact to the blueprint definition.
    - c. Publish the blueprint definition.
  3. Assign the `secure-hybrid-vnet` blueprint definition to any subscriptions requiring on-premises connectivity. This definition should be assigned in addition to the `governance-baseline` blueprint definition.

One of the biggest concerns raised by IT security and traditional governance teams is the risk that early stage cloud adoption will compromise existing assets. The above approach allows cloud adoption teams to build and migrate hybrid solutions, with reduced risk to on-premises assets. As trust in the cloud environment increases, later evolutions may remove this temporary solution.

#### NOTE

The above is a starting point to quickly create a baseline governance MVP. This is only the beginning of the governance journey. Further evolution will be needed as the company continues to adopt the cloud and takes on more risk in the following areas:

- Mission-critical workloads
- Protected data
- Cost management
- Multicloud scenarios

Moreover, the specific details of this MVP are based on the example journey of a fictional company, described in the articles that follow. We highly recommend becoming familiar with the other articles in this series before implementing this best practice.

## Iterative governance improvements

Once this MVP has been deployed, additional layers of governance can be incorporated into the environment quickly. Here are some ways to improve the MVP to meet specific business needs:

- [Security baseline for protected data](#)
- [Resource configurations for mission-critical applications](#)
- [Controls for cost management](#)
- [Controls for multicloud evolution](#)

## What does this guidance provide?

In the MVP, practices and tools from the [Deployment Acceleration discipline](#) are established to quickly apply corporate policy. In particular, the MVP uses Azure Blueprints, Azure Policy, and Azure management groups to apply a few basic corporate policies, as defined in the narrative for this fictional company. Those corporate policies are applied using Resource Manager templates and Azure policies to establish a small baseline for

identity and security.



## Incremental improvement of governance practices

Over time, this governance MVP will be used to improve governance practices. As adoption advances, business risk grows. Various disciplines within the Cloud Adoption Framework governance model will change to manage those risks. Later articles in this series discuss the incremental improvement of corporate policy affecting the fictional company. These improvements happen across three disciplines:

- The Cost Management discipline, as adoption scales.
- The Security Baseline discipline, as protected data is deployed.
- The Resource Consistency discipline, as IT operations begins supporting mission-critical workloads.



## Next steps

Now that you're familiar with the governance MVP and have an idea of the governance improvements to follow, read the supporting narrative for additional context.

[Read the supporting narrative](#)

# Standard enterprise governance guide: The narrative behind the governance strategy

11/9/2020 • 2 minutes to read • [Edit Online](#)

The following narrative describes the use case for governance during a [standard enterprise's cloud adoption journey](#). Before implementing the journey, it's important to understand the assumptions and rationale that are reflected in this narrative. Then you can better align the governance strategy to your organization's journey.

## Back story

The board of directors started the year with plans to energize the business in several ways. They're pushing leadership to improve customer experiences to gain market share. They're also pushing for new products and services that will position the company as a thought leader in the industry. They also initiated a parallel effort to reduce waste and cut unnecessary costs. Though intimidating, the actions of the board and leadership show that this effort is focusing as much capital as possible on future growth.

In the past, the company's CIO has been excluded from these strategic conversations. Because the future vision is intrinsically linked to technical growth, IT has a seat at the table to help guide these big plans. IT is now expected to deliver in new ways. The team isn't prepared for these changes and is likely to struggle with the learning curve.

## Business characteristics

The company has the following business profile:

- All sales and operations reside in a single country, with a low percentage of global customers.
- The business operates as a single business unit, with budget aligned to functions, including sales, marketing, operations, and IT.
- The business views most of IT as a capital drain or a cost center.

## Current state

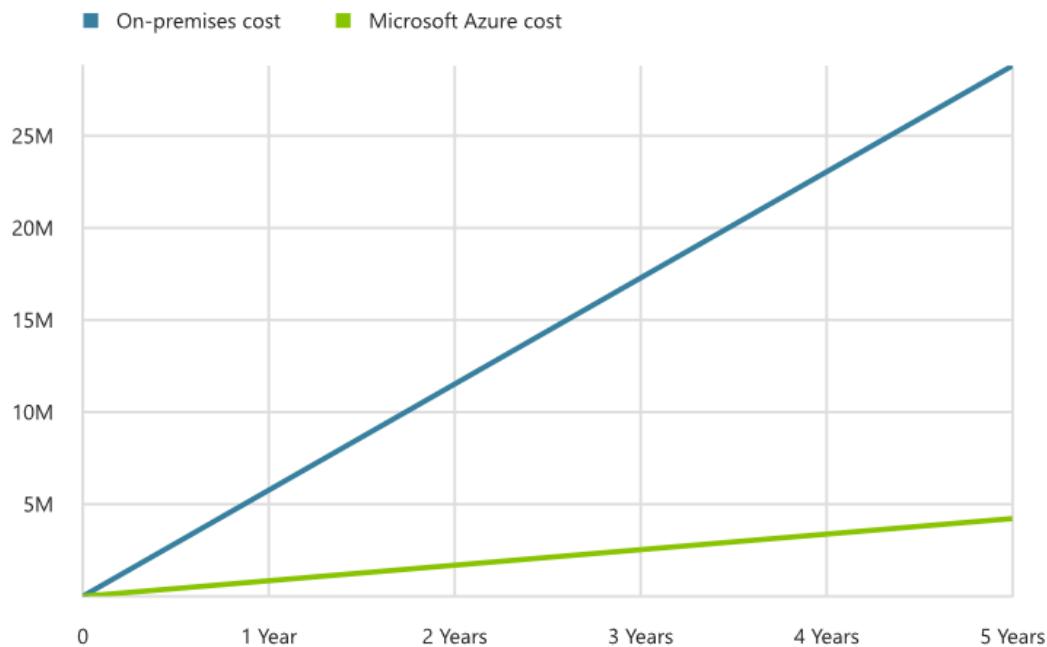
Here is the current state of the company's IT and cloud operations:

- IT operates two hosted infrastructure environments. One environment contains production assets. The second environment contains disaster recovery and some dev/test assets. These environments are hosted by two different providers. IT refers to these two datacenters as *Prod* and *DR* respectively.
- IT entered the cloud by migrating all end-user email accounts to Microsoft 365. This migration was completed six months ago. Few other IT assets have been deployed to the cloud.
- The application development teams are working in a dev/test capacity to learn about cloud-native capabilities.
- The business intelligence (BI) team is experimenting with big data in the cloud and curation of data on new platforms.
- The company has a loosely defined policy stating that personal customer data and financial data cannot be hosted in the cloud, which limits mission-critical applications in the current deployments.
- IT investments are controlled largely by capital expense. Those investments are planned yearly. In the past several years, investments have included little more than basic maintenance requirements.

## Future state

The following changes are anticipated over the next several years:

- The CIO is reviewing the policy on personal data and financial data to allow for the future state goals.
- The application development and BI teams want to release cloud-based solutions to production over the next 24 months based on the vision for customer engagement and new products.
- This year, the IT team will finish retiring the disaster recovery workloads of the DR datacenter by migrating 2,000 VMs to the cloud. This is expected to produce an estimated \$25m USD cost savings over the next five years.



- The company plans to change how it makes IT investments by repositioning the committed capital expense as an operating expense within IT. This change will provide greater cost control and enable IT to accelerate other planned efforts.

## Next steps

The company has developed a corporate policy to shape the governance implementation. The corporate policy drives many of the technical decisions.

[Review the initial corporate policy](#)

# Standard enterprise governance guide: Initial corporate policy behind the governance strategy

11/9/2020 • 4 minutes to read • [Edit Online](#)

The following corporate policy defines an initial governance position, which is the starting point for this guide. This article defines early-stage risks, initial policy statements, and early processes to enforce policy statements.

## NOTE

The corporate policy is not a technical document, but it drives many technical decisions. The governance MVP described in the [overview](#) ultimately derives from this policy. Before implementing a governance MVP, your organization should develop a corporate policy based on your own objectives and business risks.

## Cloud governance team

In this narrative, the cloud governance team is comprised of two systems administrators who have recognized the need for governance. Over the next several months, they will inherit the job of cleaning up the governance of the company's cloud presence, earning them the title of *cloud custodians*. In subsequent iterations, this title will likely change.

## Objective

The initial objective is to establish a foundation for governance agility. An effective Governance MVP allows the governance team to stay ahead of cloud adoption and implement guardrails as the adoption plan changes.

## Business risks

The company is at an early stage of cloud adoption, experimenting and building proofs of concept. Risks are now relatively low, but future risks are likely to have a significant impact. There is little definition around the final state of the technical solutions to be deployed to the cloud. In addition, the cloud readiness of IT employees is low. A foundation for cloud adoption will help the team safely learn and grow.

**Future-proofing:** There is a risk of not empowering growth, but also a risk of not providing the right protections against future risks.

An agile yet robust governance approach is needed to support the board's vision for corporate and technical growth. Failure to implement such a strategy will slow technical growth, potentially risking current and future market share growth. The impact of such a business risk is unquestionably high. However, the role IT will play in those potential future states is unknown, making the risk associated with current IT efforts relatively high. That said, until more concrete plans are aligned, the business has a high tolerance for risk.

This business risk can be broken down tactically into several technical risks:

- Well-intended corporate policies could slow transformation efforts or break critical business processes, if not considered within a structured approval flow.
- The application of governance to deployed assets could be difficult and costly.
- Governance may not be properly applied across an application or workload, creating gaps in security.
- With so many teams working in the cloud, there is a risk of inconsistency.
- Costs may not properly align to business units, teams, or other budgetary management units.

- The use of multiple identities to manage various deployments could lead to security issues.
- Despite current policies, there is a risk that protected data could be mistakenly deployed to the cloud.

## Tolerance indicators

The current tolerance for risk is high and the appetite for investing in cloud governance is low. As such, the tolerance indicators act as an early warning system to trigger more investment of time and energy. If and when the following indicators are observed, you should iteratively improve the governance strategy.

- **Cost management:** The scale of deployment exceeds predetermined limits on number of resources or monthly cost.
- **Security baseline:** Inclusion of protected data in defined cloud adoption plans.
- **Resource consistency:** Inclusion of any mission-critical applications in defined cloud adoption plans.

## Policy statements

The following policy statements establish the requirements needed to remediate the defined risks. These policies define the functional requirements for the governance MVP. Each will be represented in the implementation of the governance MVP.

Cost Management:

- For tracking purposes, all assets must be assigned to an application owner within one of the core business functions.
- When cost concerns arise, additional governance requirements will be established with the finance team.

Security Baseline:

- Any asset deployed to the cloud must have an approved data classification.
- No assets identified with a protected level of data may be deployed to the cloud, until sufficient requirements for security and governance can be approved and implemented.
- Until minimum network security requirements can be validated and governed, cloud environments are seen as perimeter networks and should meet similar connection requirements to other datacenters or internal networks.

Resource Consistency:

- Because no mission-critical workloads are deployed at this stage, there are no SLA, performance, or BCDR requirements to be governed.
- When mission-critical workloads are deployed, additional governance requirements will be established with IT operations.

Identity Baseline:

- All assets deployed to the cloud should be controlled using identities and roles approved by current governance policies.
- All groups in the on-premises Active Directory infrastructure that have elevated privileges should be mapped to an approved RBAC role.

Deployment Acceleration:

- All assets must be grouped and tagged according to defined grouping and tagging strategies.
- All assets must use an approved deployment model.
- Once a governance foundation has been established for a cloud provider, any deployment tooling must be compatible with the tools defined by the governance team.

## Processes

No budget has been allocated for ongoing monitoring and enforcement of these governance policies. Because of that, the cloud governance team has improvised ways to monitor adherence to policy statements.

- **Education:** The cloud governance team is investing time to educate the cloud adoption teams on the governance guides that support these policies.
- **Deployment reviews:** Before deploying any asset, the cloud governance team will review the governance guide with the cloud adoption teams.

## Next steps

This corporate policy prepares the cloud governance team to implement the governance MVP, which will be the foundation for adoption. The next step is to implement this MVP.

[Best practices explained](#)

# Standard enterprise governance guide: Best practices explained

11/9/2020 • 10 minutes to read • [Edit Online](#)

The governance guide starts with a set of initial **corporate policies**. These policies are used to establish a governance MVP that reflects **best practices**.

In this article, we discuss the high-level strategies that are required to create a governance MVP. The core of the governance MVP is the **Deployment Acceleration discipline**. The tools and patterns applied at this stage will enable the incremental improvements needed to expand governance in the future.

## Governance MVP (initial governance foundation)

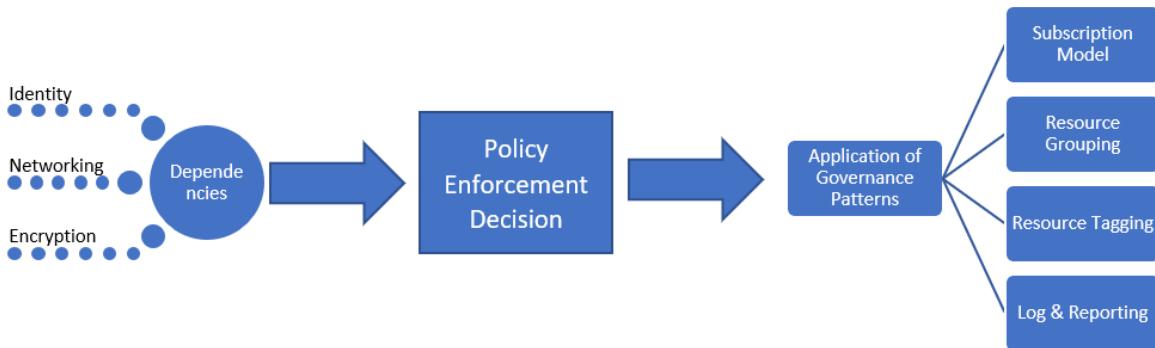
Rapid adoption of governance and corporate policy is achievable, thanks to a few simple principles and cloud-based governance tooling. These are the first three disciplines to approach in any governance process. Each discipline will be further described in this article.

To establish the starting point, this article discusses the high-level strategies behind the Security Baseline, Identity Baseline, and Deployment Acceleration disciplines that are required to create a governance MVP, which will serve as the foundation for all adoption.



## Implementation process

The implementation of the governance MVP has dependencies on identity, security, and networking. Once the dependencies are resolved, the cloud governance team will decide a few aspects of governance. The decisions from the cloud governance team and from supporting teams will be implemented through a single package of enforcement assets.



This implementation can also be described using a simple checklist:

1. Solicit decisions regarding core dependencies: identity, networking, monitoring, and encryption.
2. Determine the pattern to be used during corporate policy enforcement.
3. Determine the appropriate governance patterns for the resource consistency, resource tagging, and logging and reporting disciplines.
4. Implement the governance tools aligned to the chosen policy enforcement pattern to apply the dependent decisions and governance decisions.

## Dependent decisions

The following decisions come from teams outside of the cloud governance team. The implementation of each will come from those same teams. However, the cloud governance team is responsible for implementing a solution to validate that those implementations are consistently applied.

### Identity Baseline

Identity Baseline is the fundamental starting point for all governance. Before attempting to apply governance, identity must be established. The established identity strategy will then be enforced by the governance solutions. In this governance guide, the Identity Management team implements the [Directory Synchronization](#) pattern:

- RBAC will be provided by Azure Active Directory (Azure AD), using the directory synchronization or "Same Sign-On" that was implemented during company's migration to Microsoft 365. For implementation guidance, see [Reference Architecture for Azure AD Integration](#).
- The Azure AD tenant will also govern authentication and access for assets deployed to Azure.

In the governance MVP, the governance team will enforce application of the replicated tenant through subscription governance tooling, discussed later in this article. In future iterations, the governance team could also enforce rich tooling in Azure AD to extend this capability.

### Security Baseline: Networking

Software Defined Network is an important initial aspect of the Security Baseline. Establishing the governance MVP depends on early decisions from the Security Management team to define how networks can be safely configured.

Given the lack of requirements, IT security is playing it safe and requires a [Cloud DMZ](#) pattern. That means governance of the Azure deployments themselves will be very light.

- Azure subscriptions may connect to an existing datacenter via VPN, but must follow all existing on-premises IT governance policies regarding connection of a perimeter network to protected resources. For implementation guidance regarding VPN connectivity, see [On-premises network connected to Azure using a VPN gateway](#).
- Decisions regarding subnet, firewall, and routing are currently being deferred to each application/workload lead.
- Additional analysis is required before releasing of any protected data or mission-critical workloads.

In this pattern, cloud networks can only connect to on-premises resources over an existing VPN that is compatible

with Azure. Traffic over that connection will be treated like any traffic coming from a perimeter network. Additional considerations may be required on the on-premises edge device to securely handle traffic from Azure.

The cloud governance team has proactively invited members of the networking and IT security teams to regular meetings, in order to stay ahead of networking demands and risks.

### **Security Baseline: Encryption**

Encryption is another fundamental decision within the Security Baseline discipline. Because the company currently does not yet store any protected data in the cloud, the Security Team has decided on a less aggressive pattern for encryption. At this point, a [cloud-native pattern for encryption](#) is suggested but not required of any development team.

- No governance requirements have been set regarding the use of encryption, because the current corporate policy does not permit mission-critical or protected data in the cloud.
- Additional analysis will be required before releasing any protected data or mission-critical workloads.

## **Policy enforcement**

The first decision to make regarding Deployment Acceleration is the pattern for enforcement. In this narrative, the governance team decided to implement the [Automated Enforcement](#) pattern.

- Azure Security Center will be made available to the security and identity teams to monitor security risks. Both teams are also likely to use Security Center to identify new risks and improve corporate policy.
- RBAC is required in all subscriptions to govern authentication enforcement.
- Azure Policy will be published to each management group and applied to all subscriptions. However, the level of policies being enforced will be very limited in this initial Governance MVP.
- Although Azure management groups are being used, a relatively simple hierarchy is expected.
- Azure Blueprints will be used to deploy and update subscriptions by applying RBAC requirements, Resource Manager Templates, and Azure Policy across management groups.

## **Apply the dependent patterns**

The following decisions represent the patterns to be enforced through the policy enforcement strategy above:

**Identity Baseline.** Azure Blueprints will set RBAC requirements at a subscription level to ensure that consistent identity is configured for all subscriptions.

**Security Baseline: Networking.** The cloud governance team maintains a Resource Manager template for establishing a VPN gateway between Azure and the on-premises VPN device. When an application team requires a VPN connection, the cloud governance team will apply the gateway Resource Manager template via Azure Blueprints.

**Security Baseline: Encryption.** At this point, no policy enforcement is required in this area. This will be revisited during later iterations.

## **Application of governance-defined patterns**

The cloud governance team is responsible for the following decisions and implementations. Many require inputs from other teams, but the cloud governance team is likely to own both the decision and the implementation. The following sections outline the decisions made for this use case and details of each decision.

### **Subscription design**

The decision on what subscription design to use determines how Azure subscriptions get structured and how Azure management groups will be used to efficiently manage access, policies, and compliance of these subscription. In this narrative, the governance team has established subscriptions for production and

nonproduction workloads [production-and-nonproduction](#) subscription design pattern.

- Departments are not likely to be required given the current focus. Deployments are expected to be constrained within a single billing unit. At the stage of adoption, there may not even be an Enterprise Agreement to centralize billing. It's likely that this level of adoption is being managed by a single pay-as-you-go Azure subscription.
- Regardless of the use of the EA portal or the existence of an Enterprise Agreement, a subscription model should still be defined and agreed on to minimize administrative overhead beyond just billing.
- A common naming convention should be agreed on as part of the subscription design, based on the previous two points.

## Resource consistency

Resource consistency decisions determine the tools, processes, and effort required to ensure Azure resources are deployed, configured, and managed consistently within a subscription. In this narrative, [deployment consistency](#) has been chosen as the primary resource consistency pattern.

- Resource groups are created for applications using the lifecycle approach. Everything that is created, maintained, and retired together should reside a single resource group. For more information, see the [resource consistency decision guide](#).
- Azure Policy should be applied to all subscriptions from the associated management group.
- As part of the deployment process, Azure resource consistency templates for the resource group should be stored in source control.
- Each resource group is associated with a specific workload or application based on the lifecycle approach described above.
- Azure management groups enable updating governance designs as corporate policy matures.
- Extensive implementation of Azure Policy could exceed the team's time commitments and may not provide a great deal of value at this time. A simple default policy should be created and applied to each management group to enforce the small number of current cloud governance policy statements. This policy will define the implementation of specific governance requirements. Those implementations can then be applied across all deployed assets.

### IMPORTANT

Any time a resource in a resource group no longer shares the same lifecycle, it should be moved to another resource group. Examples include common databases and networking components. While they may serve the application being developed, they may also serve other purposes and should therefore exist in other resource groups.

## Resource tagging

Resource tagging decisions determine how metadata is applied to Azure resources within a subscription to support operations, management, and accounting purposes. In this narrative, the [classification](#) pattern has been chosen as the default model for resource tagging.

- Deployed assets should be tagged with:
  - Data classification
  - Criticality
  - SLA
  - Environment
- These four values will drive governance, operations, and security decisions.
- If this governance guide is being implemented for a business unit or team within a larger corporation, tagging should also include metadata for the billing unit.

## Logging and reporting

Logging and reporting decisions determine how your store log data and how the monitoring and reporting tools that keep IT staff informed on operational health are structured. In this narrative, a [cloud-native pattern](#)<sup>\*\*</sup> for logging and reporting is suggested.

## Incremental improvement of governance processes

As governance changes, some policy statements can't or shouldn't be controlled by automated tooling. Other policies will result in effort by the IT security team and the on-premises identity management team over time. To help manage new risks as they arise, the cloud governance team will oversee the following processes.

**Adoption acceleration:** The cloud governance team has been reviewing deployment scripts across multiple teams. They maintain a set of scripts that serve as deployment templates. Those templates are used by the cloud adoption and DevOps teams to define deployments more quickly. Each of those scripts contains the necessary requirements to enforce a set of governance policies with no additional effort from cloud adoption engineers. As the curators of these scripts, the cloud governance team can more quickly implement policy changes. As a result of script curation, the cloud governance team is seen as a source of adoption acceleration. This creates consistency among deployments, without strictly forcing adherence.

**Engineer training:** The cloud governance team offers bimonthly training sessions and has created two videos for engineers. These materials help engineers quickly learn the governance culture and how things are done during deployments. The team is adding training assets that show the difference between production and nonproduction deployments, so that engineers will understand how the new policies will affect adoption. This creates consistency among deployments, without strictly forcing adherence.

**Deployment planning:** Before deploying any asset containing protected data, the cloud governance team will review deployment scripts to validate governance alignment. Existing teams with previously approved deployments will be audited using programmatic tooling.

**Monthly audit and reporting:** Each month, the cloud governance team runs an audit of all cloud deployments to validate continued alignment to policy. When deviations are discovered, they're documented and shared with the cloud adoption teams. When enforcement doesn't risk a business interruption or data leak, the policies are automatically enforced. At the end of the audit, the cloud governance team compiles a report for the cloud strategy team and each cloud adoption team to communicate overall adherence to policy. The report is also stored for auditing and legal purposes.

**Quarterly policy review:** Each quarter, the cloud governance team and the cloud strategy team will review audit results and suggest changes to corporate policy. Many of those suggestions are the result of continuous improvements and the observation of usage patterns. Approved policy changes are integrated into governance tooling during subsequent audit cycles.

## Alternative patterns

If any of the patterns selected in this governance guide don't align with the reader's requirements, alternatives to each pattern are available:

- [Encryption patterns](#)
- [Identity patterns](#)
- [Logging and reporting patterns](#)
- [Policy enforcement patterns](#)
- [Resource consistency patterns](#)
- [Resource tagging patterns](#)
- [Software Defined Networking patterns](#)
- [Subscription design patterns](#)

## Next steps

Once this guide is implemented, each cloud adoption team can go forth with a sound governance foundation. At the same time, the cloud governance team will work to continuously update the corporate policies and governance disciplines.

The two teams will use the tolerance indicators to identify the next set of improvements needed to continue supporting cloud adoption. For the fictional company in this guide, the next step is improving the security baseline to support moving protected data to the cloud.

[Improve the Security Baseline discipline](#)

# Standard enterprise governance guide: Improve the Security Baseline discipline

11/9/2020 • 9 minutes to read • [Edit Online](#)

This article advances the [governance strategy narrative](#) by adding security controls that support moving protected data to the cloud.

## Advancing the narrative

IT and business leadership are happy with results from early experimentation by the IT, application development, and BI teams. To realize tangible business values from these experiments, those teams must be allowed to integrate protected data into solutions. This integration triggers changes to corporate policy. It also requires incremental improvement of the cloud governance implementations before protected data can land in the cloud.

### Changes to the cloud governance team

Given the effect of the changing narrative and support provided so far, the cloud governance team is now viewed differently. The two system administrators who started the team are now viewed as experienced cloud architects. As this narrative develops, the perception of them will shift from that of cloud custodians to more of a cloud guardian role.

The difference is subtle, but it's an important distinction when you're creating a governance-focused IT culture. A cloud custodian cleans up the messes made by innovative cloud architects. The two roles have natural friction and opposing goals. On the other hand, a cloud guardian helps keep the cloud safe so other cloud architects can move more quickly, with fewer messes. And a cloud guardian is involved in creating templates that accelerate deployment and adoption. So they're innovation accelerators in addition to being defenders of the Five Disciplines of Cloud Governance.

### Changes in the current state

At the start of this narrative, the application development teams were still working in a dev/test capacity, and the BI team was still in the experimental phase. IT operated two hosted infrastructure environments, referred to as [Prod](#) and [DR](#).

Since then, some things have changed that will affect governance:

- The application development team has implemented a CI/CD pipeline to deploy a cloud-native application with an improved user experience. That application doesn't yet interact with protected data, so it isn't production ready.
- The business intelligence team within IT actively curates data in the cloud from logistics, inventory, and third-party sources. This data is used to drive new predictions, which could shape business processes. Those predictions and insights aren't actionable until customer and financial data can be integrated into the data platform.
- The IT team is progressing on the CIO and CFO plans to retire the DR datacenter. More than 1,000 of the 2,000 assets in the DR datacenter have been retired or migrated.
- The loosely defined policies for personal data and financial data have been modernized. The new corporate policies are contingent on the implementation of related security and governance policies. Teams are still stalled.

### Incrementally improve the future state

Early experiments by the application development and BI teams show potential improvements in customer

experiences and data-driven decisions. Both teams want to expand adoption of the cloud over the next 18 months by deploying those solutions to production.

During the remaining six months, the cloud governance team will implement security and governance requirements to allow the cloud adoption teams to migrate the protected data in those datacenters.

The changes to current and future state expose new risks that require new policy statements.

## Changes in tangible risks

**Data breach:** When you adopt any new data platform, there's an inherent increase in liabilities related to potential data breaches. Technicians adopting cloud technologies have increased responsibility to implement solutions that can reduce this risk. A robust security and governance strategy must be implemented to ensure those technicians fulfill those responsibilities.

This business risk can be expanded into a few technical risks:

- Mission-critical applications or protected data might be deployed unintentionally.
- Protected data might be exposed during storage because of poor encryption decisions.
- Unauthorized users might access protected data.
- External intrusion might result in access to protected data.
- External intrusion or denial-of-service attacks might cause a business interruption.
- Organization or employment changes might allow unauthorized access to protected data.
- New exploits could create new intrusion or access opportunities.
- Inconsistent deployment processes might result in security gaps, which could lead to data leaks or interruptions.
- Configuration drift or missed patches might result in unintended security gaps, which could lead to data leaks or interruptions.

**Data loss:** There's also an inherent risk of data loss in the new platform. The security and governance strategy should consider the following scenarios in which data loss can happen:

- A mission-critical resource is lost or deleted.
- A mission-critical resource is present, but the data is lost because of accidental deletion.
- A mission-critical resource is present, but the data is lost because of malicious administration.

## Incremental improvement of policy statements

The following changes to policy will help remediate the new risks and guide implementation. The list looks long, but adopting these policies might be easier than you think.

- All deployed assets must be categorized by criticality and data classification. The cloud governance team and the application owner must review these classifications before deployment to the cloud.
- Applications that store or access protected data must be managed differently than applications that don't. At a minimum, they should be segmented to avoid unintended access of protected data.
- All protected data must be encrypted when at rest. This encryption is the default for all Azure Storage accounts. But you might need additional encryption strategies, including encryption of the data within the storage account, encryption of VMs, and database-level encryption when you use SQL in a VM (TDE and column encryption).
- Mission-critical data can be deleted accidentally. You need to develop a data backup strategy to handle this risk and restore the data from before the deletion point. A malicious admin can delete the mission-critical data and its backups as well. To handle this scenario, deletions of backup data should be soft deletions that can be reversed. Azure Backup can help with both of these scenarios.
- Elevated permissions in any segment that contains protected data should be an exception. Any such exceptions

will be recorded with the cloud governance team and audited regularly.

- Network subnets that contain protected data must be isolated from other subnets. Network traffic between protected data subnets will be audited regularly.
- No subnet that contains protected data should be directly accessible over the public internet or across datacenters. Access to those subnets must be routed through intermediate subnets. All access into those subnets must come through a firewall solution that can perform packet scanning and blocking functions.
- Governance tooling must audit and enforce network configuration requirements defined by the security management team.
- Governance tooling must limit VM deployment to only approved images.
- Governance process must validate that backup, recovery, and SLA adherence are properly implemented for mission-critical applications and protected data.
- Whenever possible, node configuration management should apply policy requirements to the configuration of any guest operating system.
- Governance tooling must enforce that automatic updates are enabled on all deployed assets. Violations must be reviewed with operational management teams and remediated in accordance with operations policies. Assets that aren't automatically updated must be included in processes owned by IT operations.
- Creation of new subscriptions or management groups for any mission-critical applications or protected data will require a review from the cloud governance team to ensure that the proper blueprint is assigned.
- A least-privilege access model will be applied to any management group or subscription that contains mission-critical applications or protected data.
- Trends and exploits that could affect cloud deployments should be reviewed regularly by the security team to provide updates to security management tooling used in the cloud.
- Deployment tooling must be approved by the cloud governance team to ensure ongoing governance of deployed assets.
- Deployment scripts must be maintained in a central repository accessible by the cloud governance team for periodic review and auditing.
- Governance processes must include audits at the point of deployment and at regular cycles to ensure consistency across all assets.
- Deployment of any applications that require customer authentication must use an approved identity provider that's compatible with the primary identity provider for internal users.
- Cloud governance processes must include quarterly reviews with identity management teams. These reviews can help identify malicious actors or usage patterns that should be prevented by cloud asset configuration.

## Incremental improvement of governance practices

The governance MVP design will change to include new Azure policies and an implementation of Azure Cost Management + Billing. Together, these two design changes will fulfill the new corporate policy statements.

- The networking and IT security teams will define network requirements. The cloud governance team will support the conversation.
- The identity and IT security teams will define identity requirements and make any necessary changes to local Active Directory implementation. The cloud governance team will review changes.
- Create a repository in Azure DevOps to store and version all relevant Azure Resource Manager templates and scripted configurations.
- Azure Recovery Services vault implementation:
  - Define and deploy an Azure Recovery Services vault for backup and recovery processes.
  - Create a Resource Manager template for creation of a vault in each subscription.
- Azure Security Center implementation:
  - Configure Azure Security Center for any management group that contains protected data classifications.
  - Set automatic provisioning to on by default to ensure patching compliance.

- Establish OS security configurations. The IT security team will define the configuration.
- Support the IT security team in the initial use of Security Center. Transition the use of Security Center to the IT security team, but maintain access for the purpose of continually improving governance.
- Create a Resource Manager template that reflects the changes required for Security Center configuration within a subscription.
- Update Azure policies for all subscriptions:
  - Audit and enforce the criticality of data and data classification across all management groups and subscriptions to identify any subscriptions with protected data classifications.
  - Audit and enforce the use of approved images only.
- Update Azure policies for all subscriptions that contain protected data classifications:
  - Audit and enforce the use of standard Azure RBAC roles only.
  - Audit and enforce encryption for all storage accounts and files at rest on individual nodes.
  - Audit and enforce the application of an NSG to all NICs and subnets. The networking and IT security teams will define the NSG.
  - Audit and enforce the use of approved network subnet and virtual network per network interface.
  - Audit and enforce the limitation of user-defined routing tables.
  - Apply the built-in policies for guest configuration as follows:
    - Audit that Windows web servers are using secure communication protocols.
    - Audit that password security settings are set correctly inside Linux and Windows machines.
    - Audit and enforce that Azure Recovery Services vaults exist in the subscription.
- Firewall configuration:
  - Identify a configuration of Azure Firewall that meets necessary security requirements. Alternatively, identify a compatible third-party appliance that's compatible with Azure. The Azure Security Benchmark provides additional information on [network security strategy](#) and [firewall configurations to support your security strategy](#).
  - Create a Resource Manager template to deploy the firewall with required configurations.
- Azure Blueprints:
  - Create a new blueprint named `protected-data`.
  - Add the Azure Firewall templates, Azure Security Center templates, and Azure Recovery Services vault templates to the blueprint.
  - Add the new policies for protected data subscriptions.
  - Publish the blueprint to any management group that currently plans on hosting protected data.
  - Apply the new blueprint to each affected subscription and to existing blueprints.

## Conclusion

Adding the above processes and changes to the governance MVP will help to remediate many of the risks associated with security governance. Together, they add the network, identity, and security monitoring tools needed to protect data.

## Next steps

As cloud adoption continues and delivers additional business value, risks and cloud governance needs also change. For the fictional company in this guide, the next step is to support mission-critical workloads. At this point, resource consistency controls are needed.

[Improve the Resource Consistency discipline](#)

# Standard enterprise governance guide: Improve the Resource Consistency discipline

11/9/2020 • 6 minutes to read • [Edit Online](#)

This article advances the narrative by adding resource consistency controls to support mission-critical applications.

## Advancing the narrative

New customer experiences, new prediction tools, and migrated infrastructure continue to progress. The business is now ready to begin using those assets in a production capacity.

### Changes in the current state

In the previous phase of this narrative, the application development and BI teams were nearly ready to integrate customer and financial data into production workloads. The IT team was in the process of retiring the DR datacenter.

Since then, some things have changed that will affect governance:

- IT has retired 100% of the DR datacenter, ahead of schedule. In the process, a set of assets in the production datacenter were identified as cloud migration candidates.
- The application development teams are now ready for production traffic.
- The BI team is ready to feed predictions and insights back into operation systems in the production datacenter.

### Incrementally improve the future state

Before using Azure deployments in production business processes, cloud operations must mature. In conjunction, additional governance changes are required to ensure assets can be operated properly.

The changes to current and future state expose new risks that will require new policy statements.

## Changes in tangible risks

**Business interruption:** There is an inherent risk of any new platform causing interruptions to mission-critical business processes. The IT operations team and the teams executing on various cloud adoptions are relatively inexperienced with cloud operations. This increases the risk of interruption and must be remediated and governed.

This business risk can be expanded into several technical risks:

1. External intrusion or denial of service attacks might cause a business interruption.
2. Mission-critical assets may not be properly discovered, and therefore might not be properly operated.
3. Undiscovered or mislabeled assets might not be supported by existing operational management processes.
4. The configuration of deployed assets may not meet performance expectations.
5. Logging might not be properly recorded and centralized to allow for remediation of performance issues.
6. Recovery policies may fail or take longer than expected.
7. Inconsistent deployment processes might result in security gaps that could lead to data leaks or interruptions.
8. Configuration drift or missed patches might result in unintended security gaps that could lead to data leaks or interruptions.
9. Configuration might not enforce the requirements of defined SLAs or committed recovery requirements.
10. Deployed operating systems or applications might fail to meet hardening requirements.

11. With so many teams working in the cloud, there is a risk of inconsistency.

## Incremental improvement of the policy statements

The following changes to policy will help remediate the new risks and guide implementation. The list looks long, but adopting these policies may be easier than it appears.

1. All deployed assets must be categorized by criticality and data classification. Classifications are to be reviewed by the cloud governance team and the application owner before deployment to the cloud.
2. Subnets containing mission-critical applications must be protected by a firewall solution capable of detecting intrusions and responding to attacks.
3. Governance tooling must audit and enforce network configuration requirements defined by the security management team.
4. Governance tooling must validate that all assets related to mission-critical applications or protected data are included in monitoring for resource depletion and optimization.
5. Governance tooling must validate that the appropriate level of logging data is being collected for all mission-critical applications or protected data.
6. Governance process must validate that backup, recovery, and SLA adherence are properly implemented for mission-critical applications and protected data.
7. Governance tooling must limit virtual machine deployments to approved images only.
8. Governance tooling must enforce that automatic updates are prevented on all deployed assets that support mission-critical applications. Violations must be reviewed with operational management teams and remediated in accordance with operations policies. Assets that are not automatically updated must be included in processes owned by IT operations.
9. Governance tooling must validate tagging related to cost, criticality, SLA, application, and data classification. All values must align to predefined values managed by the governance team.
10. Governance processes must include audits at the point of deployment and at regular cycles to ensure consistency across all assets.
11. Trends and exploits that could affect cloud deployments should be reviewed regularly by the security team to provide updates to security management tooling used in the cloud.
12. Before release into production, all mission-critical applications and protected data must be added to the designated operational monitoring solution. Assets that cannot be discovered by the chosen IT operations tooling, cannot be released for production use. Any changes required to make the assets discoverable must be made to the relevant deployment processes to ensure assets will be discoverable in future deployments.
13. When discovered, operational management teams will size assets, to ensure that assets meet performance requirements.
14. Deployment tooling must be approved by the cloud governance team to ensure ongoing governance of deployed assets.
15. Deployment scripts must be maintained in a central repository accessible by the cloud governance team for periodic review and auditing.
16. Governance review processes must validate that deployed assets are properly configured in alignment with SLA and recovery requirements.

## Incremental improvement of governance practices

This section of the article will change the governance MVP design to include new Azure policies and an implementation of Azure Cost Management + Billing. Together, these two design changes will fulfill the new corporate policy statements.

1. The cloud operations team will define operational monitoring tooling and automated remediation tooling. The cloud governance team will support those discovery processes. In this use case, the cloud operations team

chose Azure Monitor as the primary tool for monitoring mission-critical applications.

2. Create a repository in Azure DevOps to store and version all relevant Resource Manager templates and scripted configurations.
3. Azure Recovery Services vault implementation:
  - a. Define and deploy an Azure Recovery Services vault for backup and recovery processes.
  - b. Create a Resource Manager template for creation of a vault in each subscription.
4. Update Azure Policy for all subscriptions:
  - a. Audit and enforce criticality and data classification across all subscriptions to identify any subscriptions with mission-critical assets.
  - b. Audit and enforce the use of approved images only.
5. Azure Monitor implementation:
  - a. Once a mission-critical workload is identified, create an Azure Monitor Log Analytics workspace.
  - b. During deployment testing, the cloud operations team deploys the necessary agents and tests discovery.
6. Update Azure Policy for all subscriptions that contain mission-critical applications.
  - a. Audit and enforce the application of an NSG to all NICs and subnets. Networking and IT security define the NSG.
  - b. Audit and enforce the use of approved network subnets and virtual networks for each network interface.
  - c. Audit and enforce the limitation of user-defined routing tables.
  - d. Audit and enforce deployment of Azure Monitor agents for all virtual machines.
  - e. Audit and enforce that Azure Recovery Services vaults exist in the subscription.
7. Firewall configuration:
  - a. Identify a configuration of Azure Firewall that meets security requirements. Alternatively, identify a third-party appliance that is compatible with Azure.
  - b. Create a Resource Manager template to deploy the firewall with required configurations.
8. Azure blueprint:
  - a. Create a new Azure blueprint named `protected-data`.
  - b. Add the firewall and Azure Recovery Services vault templates to the blueprint.
  - c. Add the new policies for protected data subscriptions.
  - d. Publish the blueprint to any management group that will host mission-critical applications.
  - e. Apply the new blueprint to each affected subscription as well as existing blueprints.

## Conclusion

These additional processes and changes to the governance MVP help remediate many of the risks associated with resource governance. Together they add recovery, sizing, and monitoring controls that empower cloud-aware operations.

## Next steps

As cloud adoption continues and delivers additional business value, risks and cloud governance needs will also change. For the fictional company in this guide, the next trigger is when the scale of deployment exceeds 100 assets to the cloud or monthly spending exceeds \$1,000 per month. At this point, the cloud governance team adds cost management controls.

[Improve the Cost Management discipline](#)

# Standard enterprise governance guide: Improve the Cost Management discipline

11/9/2020 • 4 minutes to read • [Edit Online](#)

This article advances the narrative by adding cost controls to the governance MVP.

## Advancing the narrative

Adoption has grown beyond the cost tolerance indicator defined in the governance MVP. This is a good thing, as it corresponds with migrations from the DR datacenter. The increase in spending now justifies an investment of time from the cloud governance team.

### Changes in the current state

In the previous phase of this narrative, IT had retired 100% of the DR datacenter. The application development and BI teams were ready for production traffic.

Since then, some things have changed that will affect governance:

- The migration team has begun migrating VMs out of the production datacenter.
- The application development teams are actively pushing production applications to the cloud through CI/CD pipelines. Those applications can reactively scale with user demands.
- The business intelligence team within IT has delivered several predictive analytics tools in the cloud. The volumes of data aggregated in the cloud continues to grow.
- All of this growth supports committed business outcomes. Costs have begun to balloon. Projected budgets are growing faster than expected. The CFO needs improved approaches to managing costs.

### Incrementally improve the future state

Cost monitoring and reporting is to be added to the cloud solution. IT is still serving as a cost clearing house. This means that payment for cloud services continues to come from IT procurement. Reporting should tie direct operating expenses to the functions that are consuming the cloud costs. This model is referred to as a *showback* cloud accounting model.

The changes to current and future state expose new risks that will require new policy statements.

## Changes in tangible risks

**Budget control:** There is an inherent risk that self-service capabilities will result in excessive and unexpected costs on the new platform. Governance processes for monitoring costs and mitigating ongoing cost risks must be in place to ensure continued alignment with the planned budget.

This business risk can be expanded into a few technical risks:

- Actual costs might exceed the plan.
- Business conditions change. When they do, there will be cases when a business function needs to consume more cloud services than expected, leading to spending anomalies. There is a risk that this extra spending will be considered overages, as opposed to a necessary adjustment to the plan.
- Systems could be overprovisioned, resulting in excess spending.

## Incremental improvement of the policy statements

The following changes to policy will help remediate the new risks and guide implementation.

- All cloud costs should be monitored against plan on a weekly basis by the governance team. Reporting on deviations between cloud costs and plan is to be shared with IT leadership and finance monthly. All cloud costs and plan updates should be reviewed with IT leadership and finance monthly.
- All costs must be allocated to a business function for accountability purposes.
- Cloud assets should be continually monitored for optimization opportunities.
- Cloud governance tooling must limit asset sizing options to an approved list of configurations. The tooling must ensure that all assets are discoverable and tracked by the cost monitoring solution.
- During deployment planning, any required cloud resources associated with the hosting of production workloads should be documented. This documentation will help refine budgets and prepare additional automation to prevent the use of more expensive options. During this process consideration should be given to different discounting tools offered by the cloud provider, such as reserved instances or license cost reductions.
- All application owners are required to attend trained on practices for optimizing workloads to better control cloud costs.

## Incremental improvement of best practices

This section of the article will change the governance MVP design to include new Azure policies and an implementation of Azure Cost Management + Billing. Together, these two design changes will fulfill the new corporate policy statements.

1. Implement Azure Cost Management + Billing.
  - a. Establish the right scope of access to align with the subscription pattern and the Resource Consistency discipline. Assuming alignment with the governance MVP defined in prior articles, this requires **enrollment account scope** access for the cloud governance team executing on high-level reporting. Additional teams outside of governance may require **resource group scope** access.
  - b. Establish a budget in Azure Cost Management + Billing.
  - c. Review and act on initial recommendations. Have a recurring process to support reporting.
  - d. Configure and execute Azure Cost Management + Billing reporting, both initial and recurring.
2. Update Azure Policy
  - a. Audit the tagging, management group, subscription, and resource group values to identify any deviation.
  - b. Establish SKU size options to limit deployments to SKUs listed in deployment planning documentation.

## Conclusion

Adding these processes and changes to the governance MVP helps remediate many of the risks associated with cost governance. Together, they create the visibility, accountability, and optimization needed to control costs.

## Next steps

As cloud adoption continues and delivers additional business value, risks and cloud governance needs will also change. For the fictional company in this guide, the next step is using this governance investment to manage multiple clouds.

[Multicloud evolution](#)

# Standard enterprise governance guide: Multicloud improvement

11/9/2020 • 4 minutes to read • [Edit Online](#)

This article advances the narrative by adding controls for multicloud adoption.

## Advancing the narrative

Microsoft recognizes that customers may adopt multiple clouds for specific purposes. The fictional customer in this guide is no exception. In parallel with their Azure adoption journey, business success has led to the acquisition of a small but complementary business. That business is running all of their IT operations on a different cloud provider.

This article describes how things change when integrating the new organization. For purposes of the narrative, we assume this company has completed each of the governance iterations outlined in this governance guide.

### Changes in the current state

In the previous phase of this narrative, the company had begun actively pushing production applications to the cloud through CI/CD pipelines.

Since then, some things have changed that will affect governance:

- Identity is controlled by an on-premises instance of Active Directory. Hybrid identity is facilitated through replication to Azure Active Directory.
- IT operations or cloud operations are largely managed by Azure Monitor and related automated processes.
- Disaster recovery and business continuity is controlled by Azure Recovery Services vaults.
- Azure Security Center is used to monitor security violations and attacks.
- Azure Security Center and Azure Monitor are both used to monitor governance of the cloud.
- Azure Blueprints, Azure Policy, and Azure management groups are used to automate compliance with policy.

### Incrementally improve the future state

The goal is to integrate the acquisition company into existing operations wherever possible.

## Changes in tangible risks

**Business acquisition cost:** Acquisition of the new business is estimated to be profitable in approximately five years. Because of the slow rate of return, the board wants to control acquisition costs, as much as possible. There is a risk of cost control and technical integration conflicting with one another.

This business risk can be expanded into a few technical risks:

- Cloud migration might produce additional acquisition costs.
- The new environment might not be properly governed, which could result in policy violations.

## Incremental improvement of the policy statements

The following changes to policy will help remediate the new risks and guide implementation:

- All assets in a secondary cloud must be monitored through existing operational management and security monitoring tools.

- All organization units must be integrated into the existing identity provider.
- The primary identity provider should govern authentication to assets in the secondary cloud.

## Incremental improvement of governance practices

This section of the article will change the governance MVP design to include new Azure policies and an implementation of Azure Cost Management + Billing. Together, these design changes will fulfill the new corporate policy statements.

1. Connect the networks. This step is executed by the networking and IT security teams, and supported by the cloud governance team. Adding a connection from the MPLS/leased-line provider to the new cloud will integrate networks. Adding routing tables and firewall configurations will control access and traffic between the environments.
2. Consolidate identity providers. Depending on the workloads being hosted in the secondary cloud, there are a variety of options to identity provider consolidation. The following are a few examples:
  - a. For applications that authenticate using OAuth 2, users from Active Directory in the secondary cloud can simply be replicated to the existing Azure AD tenant. This ensures all users can be authenticated in the tenant.
  - b. At the other extreme, federation allows OUs to flow into Active Directory on-premises, then into the Azure AD instance.
3. Add assets to Azure Site Recovery.
  - a. Azure Site Recovery was designed from the beginning as a hybrid or multicloud tool.
  - b. VMs in the secondary cloud might be able to be protected by the same Azure Site Recovery processes used to protect on-premises assets.
4. Add assets to Azure Cost Management + Billing.
  - a. Azure Cost Management + Billing was designed from the beginning as a multicloud tool.
  - b. Virtual machines in the secondary cloud may be compatible with Azure Cost Management + Billing for some cloud providers. Additional costs may apply.
5. Add assets to Azure Monitor.
  - a. Azure Monitor was designed as a hybrid cloud tool from inception.
  - b. Virtual machines in the secondary cloud may be compatible with Azure Monitor agents, allowing them to be included in Azure Monitor for operational monitoring.
6. Adopt governance enforcement tools.
  - a. Governance enforcement is cloud-specific.
  - b. The corporate policies established in the governance guide are not cloud-specific. While the implementation may vary from cloud to cloud, the policies can be applied to the secondary provider.

Multicloud adoption should be contained to where it is required based on technical needs or specific business requirements. As multicloud adoption grows, so does complexity and security risks.

## Conclusion

This series of articles described the incremental development of governance best practices, aligned with the experiences of this fictional company. By starting small, but with the right foundation, the company could move quickly and yet still apply the right amount of governance at the right time. The MVP by itself did not protect the customer. Instead, it created the foundation to manage risks and add protections. From there, layers of governance were applied to remediate tangible risks. The exact journey presented here won't align 100% with the experiences of any reader. Rather, it serves as a pattern for incremental governance. You should mold these best practices to fit your own unique constraints and governance requirements.

# Governance guide for complex enterprises

11/9/2020 • 8 minutes to read • [Edit Online](#)

## Overview of best practices

This governance guide follows the experiences of a fictional company through various stages of governance maturity. It is based on real customer experiences. The suggested best practices are based on the constraints and needs of the fictional company.

As a quick starting point, this overview defines a minimum viable product (MVP) for governance based on best practices. It also provides links to some governance improvements that add further best practices as new business or technical risks emerge.

### WARNING

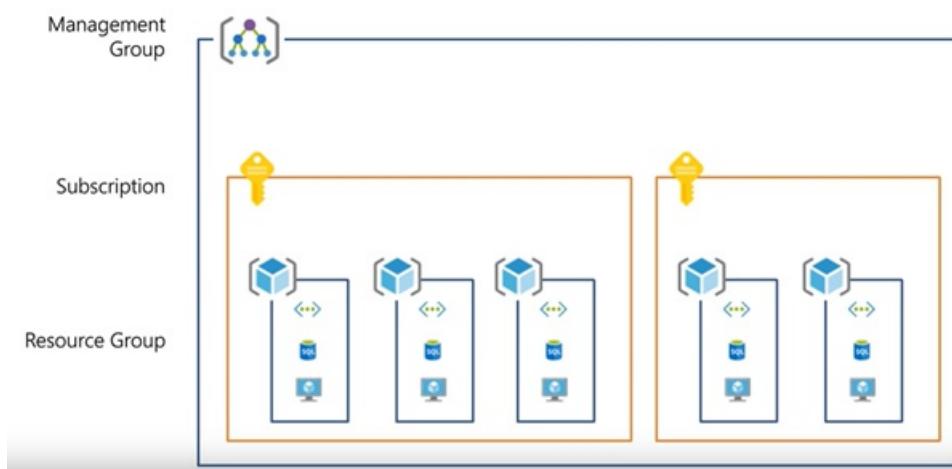
This MVP is a baseline starting point, based on a set of assumptions. Even this minimal set of best practices is based on corporate policies that are driven by unique business risks and risk tolerances. To see whether these assumptions apply to you, read the [longer narrative](#) that follows this article.

## Governance best practices

These best practices serve as a foundation for an organization to quickly and consistently add governance guardrails across multiple Azure subscriptions.

### Resource organization

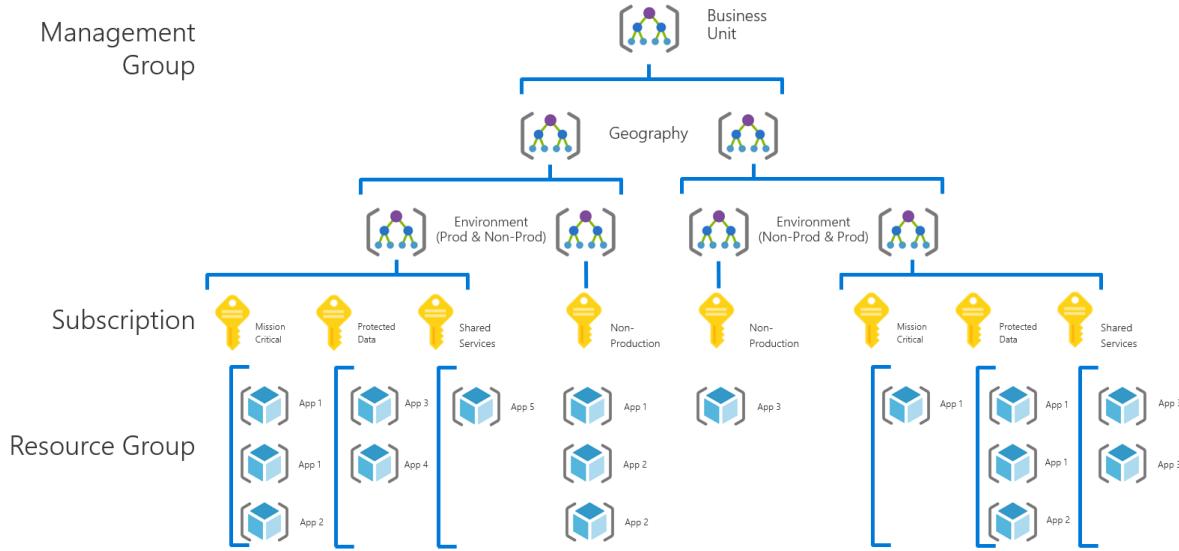
The following diagram shows the governance MVP hierarchy for organizing resources.



Every application should be deployed in the proper area of the management group, subscription, and resource group hierarchy. During deployment planning, the cloud governance team will create the necessary nodes in the hierarchy to empower the cloud adoption teams.

1. Define a management group for each business unit with a detailed hierarchy that reflects geography first, then environment type (for example, production or nonproduction environments).
2. Create a production subscription and a nonproduction subscription for each unique combination of discrete business unit or geography. Creating multiple subscriptions requires careful consideration. For more information, see the [subscription decision guide](#).
3. Apply [consistent nomenclature](#) at each level of this grouping hierarchy.

- Resource groups should be deployed in a manner that considers its contents lifecycle. Resources that are developed together, managed together, and retired together belong in the same resource group. For more information about best practices for using resource groups, see the [resource consistency decision guide](#).
- Region selection** is incredibly important and must be considered so that networking, monitoring, auditing can be in place for failover/failback as well as confirmation that [needed SKUs are available in the preferred regions](#).



These patterns provide room for growth without making the hierarchy needlessly complicated.

#### NOTE

In the event of changes to your business requirements, Azure management groups allow you to easily reorganize your management hierarchy and subscription group assignments. However, keep in mind that policy and role assignments applied to a management group are inherited by all subscriptions underneath that group in the hierarchy. If you plan to reassign subscriptions between management groups, make sure that you are aware of any policy and role assignment changes that may result. See the [Azure management groups documentation](#) for more information.

## Governance of resources

A set of global policies and RBAC roles will provide a baseline level of governance enforcement. To meet the cloud governance team's policy requirements, implementing the governance MVP requires completing the following tasks:

- Identify the Azure Policy definitions needed to enforce business requirements. This might include using built-in definitions and creating new custom definitions. To keep up with the pace of newly released built-in definitions, there's an [atom feed](#) of all the commits for built-in policies, which you can use for an RSS feed. Alternatively, you can check [AzAdvertiser](#).
- Create a blueprint definition using these built-in and custom policy and the role assignments required by the governance MVP.
- Apply policies and configuration globally by assigning the blueprint definition to all subscriptions.

#### Identify policy definitions

Azure provides several built-in policies and role definitions that you can assign to any management group, subscription, or resource group. Many common governance requirements can be handled using built-in definitions. However, it's likely that you will also need to create custom policy definitions to handle your specific requirements.

Custom policy definitions are saved to either a management group or a subscription and are inherited through the management group hierarchy. If a policy definition's save location is a management group, that policy definition is available to assign to any of that group's child management groups or subscriptions.

Since the policies required to support the governance MVP are meant to apply to all current subscriptions, the following business requirements will be implemented using a combination of built-in definitions and custom definitions created in the root management group:

1. Restrict the list of available role assignments to a set of built-in Azure roles authorized by your cloud governance team. This requires a [custom policy definition](#).
2. Require the following tags on all resources: *Department/Billing Unit, Geography, Data Classification, Criticality, SLA, Environment, Application Archetype, Application, and Application Owner*. This can be handled using the `Require specified tag` built-in definition.
3. Require that the `Application` tag for resources should match the name of the relevant resource group. This can be handled using the "Require tag and its value" built-in definition.

For information on defining custom policies see the [Azure Policy documentation](#). For guidance and examples of custom policies, consult the [Azure Policy samples site](#) and the associated [GitHub repository](#).

#### Assign Azure Policy and RBAC roles using Azure Blueprints

Azure policies can be assigned at the resource group, subscription, and management group level, and can be included in [Azure Blueprints](#) definitions. Although the policy requirements defined in this governance MVP apply to all current subscriptions, it's very likely that future deployments will require exceptions or alternative policies. As a result, assigning policy using management groups, with all child subscriptions inheriting these assignments, may not be flexible enough to support these scenarios.

Azure Blueprints allows consistent assignment of policy and roles, application of Resource Manager templates, and deployment of resource groups across multiple subscriptions. Like policy definitions, blueprint definitions are saved to management groups or subscriptions. The policy definitions are available through inheritance to any children in the management group hierarchy.

The cloud governance team has decided that enforcement of required Azure Policy and RBAC assignments across subscriptions will be implemented through Azure Blueprints and associated artifacts:

1. In the root management group, create a blueprint definition named `governance-baseline`.
2. Add the following blueprint artifacts to the blueprint definition:
  - a. Policy assignments for the custom Azure Policy definitions defined at the management group root.
  - b. Resource group definitions for any groups required in subscriptions created or governed by the Governance MVP.
  - c. Standard role assignments required in subscriptions created or governed by the Governance MVP.
3. Publish the blueprint definition.
4. Assign the `governance-baseline` blueprint definition to all subscriptions.

See the [Azure Blueprints documentation](#) for more information on creating and using blueprint definitions.

#### Secure hybrid VNet

Specific subscriptions often require some level of access to on-premises resources. This is common in migration scenarios or dev scenarios where dependent resources reside in the on-premises datacenter.

Until trust in the cloud environment is fully established it's important to tightly control and monitor any allowed communication between the on-premises environment and cloud workloads, and that the on-premises network is secured against potential unauthorized access from cloud-based resources. To support these scenarios, the governance MVP adds the following best practices:

1. Establish a cloud secure hybrid VNet.

- a. The [VPN reference architecture](#) establishes a pattern and deployment model for creating a VPN Gateway in Azure.
  - b. Validate that on-premises security and traffic management mechanisms treat connected cloud networks as untrusted. Resources and services hosted in the cloud should only have access to authorized on-premises services.
  - c. Validate that the local edge device in the on-premises datacenter is compatible with [Azure VPN Gateway requirements](#) and is configured to access the public internet.
  - d. Note that VPN tunnels should not be considered production ready circuits for anything but the most simple workloads. Anything beyond a few simple workloads requiring on-premises connectivity should use Azure ExpressRoute.
2. In the root management group, create a second blueprint definition named `secure-hybrid-vnet`.
- a. Add the Resource Manager template for the VPN Gateway as an artifact to the blueprint definition.
  - b. Add the Resource Manager template for the virtual network as an artifact to the blueprint definition.
  - c. Publish the blueprint definition.
3. Assign the `secure-hybrid-vnet` blueprint definition to any subscriptions requiring on-premises connectivity. This definition should be assigned in addition to the `governance-baseline` blueprint definition.

One of the biggest concerns raised by IT security and traditional governance teams is the risk that early stage cloud adoption will compromise existing assets. The above approach allows cloud adoption teams to build and migrate hybrid solutions, with reduced risk to on-premises assets. As trust in the cloud environment increases, later evolutions may remove this temporary solution.

#### **NOTE**

The above is a starting point to quickly create a baseline governance MVP. This is only the beginning of the governance journey. Further evolution will be needed as the company continues to adopt the cloud and takes on more risk in the following areas:

- Mission-critical workloads
- Protected data
- Cost management
- Multicloud scenarios

Moreover, the specific details of this MVP are based on the example journey of a fictional company, described in the articles that follow. We highly recommend becoming familiar with the other articles in this series before implementing this best practice.

## Incremental governance improvements

Once this MVP has been deployed, additional layers of governance can be quickly incorporated into the environment. Here are some ways to improve the MVP to meet specific business needs:

- [Security baseline for protected data](#)
- [Resource configurations for mission-critical applications](#)
- [Controls for cost management](#)
- [Controls for incremental multicloud improvement](#)

## What does this guidance provide?

In the MVP, practices and tools from the [Deployment Acceleration discipline](#) are established to quickly apply corporate policy. In particular, the MVP uses Azure Blueprints, Azure Policy, and Azure management groups to apply a few basic corporate policies, as defined in the narrative for this fictional company. Those corporate policies are applied using Azure Resource Manager templates and Azure policies to establish a small baseline for

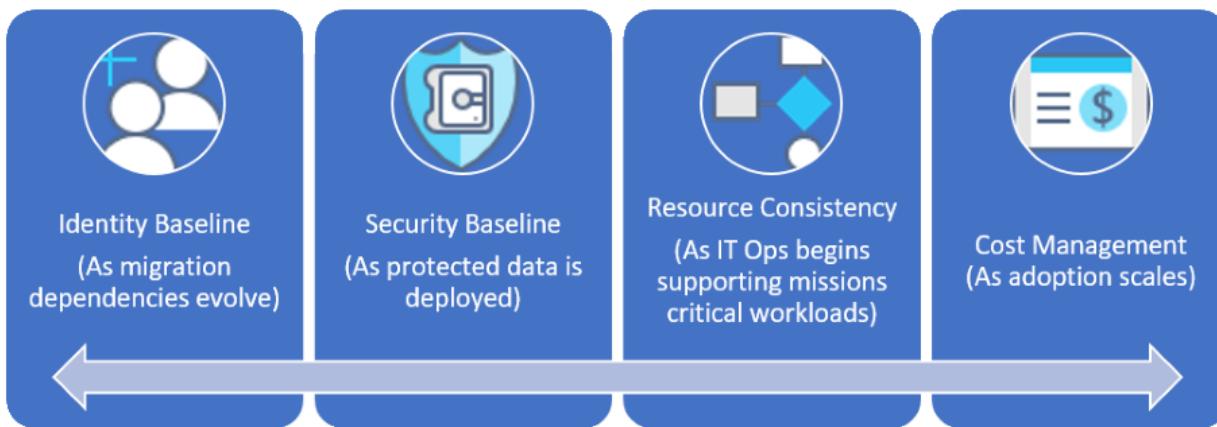
identity and security.



## Incremental improvements to governance practices

Over time, this governance MVP will be used to incrementally improve governance practices. As adoption advances, business risk grows. Various disciplines within the Cloud Adoption Framework governance model will adapt to manage those risks. Later articles in this series discuss the changes in corporate policy affecting the fictional company. These changes happen across four disciplines:

- The Identity Baseline discipline, as migration dependencies change in the narrative.
- The Cost Management discipline, as adoption scales.
- The Security Baseline discipline, as protected data is deployed.
- The Resource Consistency discipline, as IT operations begins supporting mission-critical workloads.



## Next steps

Now that you're familiar with the governance MVP and the forthcoming governance changes, read the supporting narrative for additional context.

[Read the supporting narrative](#)

# Governance guide for complex enterprises: The supporting narrative

11/9/2020 • 4 minutes to read • [Edit Online](#)

The following narrative establishes a use case for [governance during complex enterprise's cloud adoption journey](#). Before acting on the recommendations in the guide, it's important to understand the assumptions and reasoning that are reflected in this narrative. Then you can better align the governance strategy to your organization's cloud adoption journey.

## Back story

Customers are demanding a better experience when interacting with this company. The current experience caused market erosion and led to the board to hire a chief digital officer (CDO). The CDO is working with marketing and sales to drive a digital transformation that will power improved experiences. Additionally, several business units recently hired data scientists to farm data and improve many of the manual experiences through learning and prediction. IT is supporting these efforts where it can. There are "shadow IT" activities occurring that fall outside of needed governance and security controls.

The IT organization is also facing its own challenges. Finance is planning continued reductions in the IT budget over the next five years, leading to some necessary spending cuts starting this year. Conversely, GDPR and other data sovereignty requirements are forcing IT to invest in assets in additional countries to localize data. Two of the existing datacenters are overdue for hardware refreshes, causing further problems with employee and customer satisfaction. Three more datacenters require hardware refreshes during the execution of the five-year plan. The CFO is pushing the CIO to consider the cloud as an alternative for those datacenters, to free up capital expenses.

The CIO has innovative ideas that could help the company, but she and her teams are limited to fighting fires and controlling costs. At a luncheon with the CDO and one of the business unit leaders, the cloud migration conversation generated interest from the CIO's peers. The three leaders aim to support each other using the cloud to achieve their business objectives, and they have begun the exploration and planning stages of cloud adoption.

## Business characteristics

The company has the following business profile:

- Sales and operations span multiple geographic areas with global customers in multiple markets.
- The business grew through acquisition and operates across three business units based on the target customer base. Budgeting is a complex matrix across business units and functions.
- The business views most of IT as a capital drain or a cost center.

## Current state

Here is the current state of the company's IT and cloud operations:

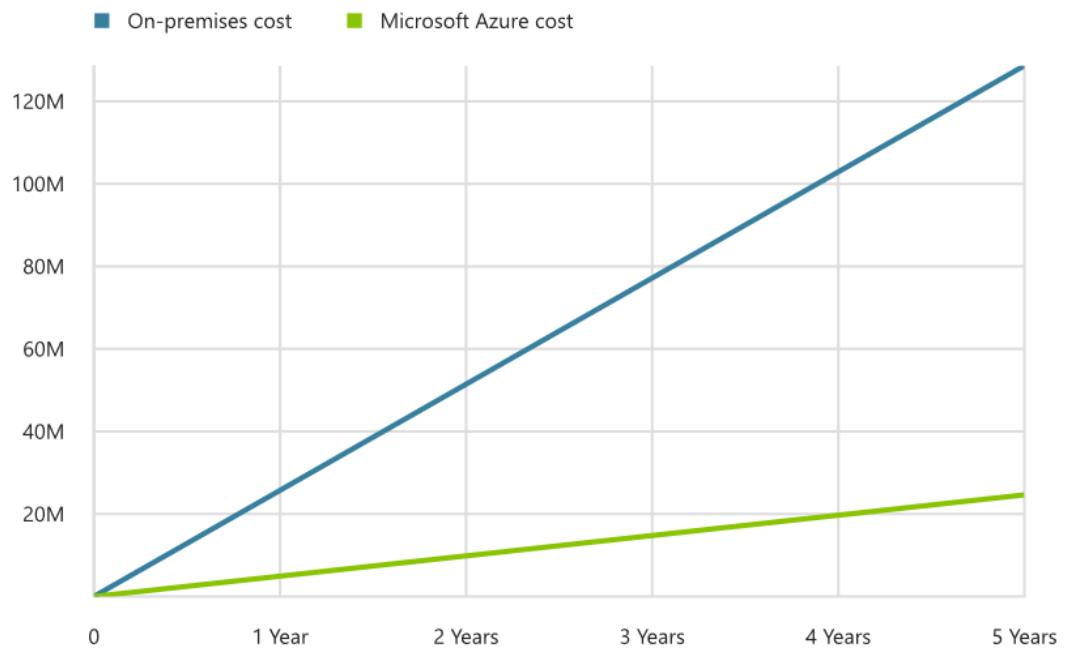
- IT operates more than 20 privately owned datacenters around the globe.
- Due to organic growth and multiple geographies, there are a few IT teams that have unique data sovereignty and compliance requirements that impact a single business unit operating within a specific geography.
- Each datacenter is connected by a series of regional leased lines, creating a loosely coupled global WAN.

- IT entered the cloud by migrating all end-user email accounts to Microsoft 365. This migration was completed more than six months ago. Since then, only a few IT assets have been deployed to the cloud.
- The CDO's primary development team is working in a dev/test capacity to learn about cloud-native capabilities.
- One business unit is experimenting with big data in the cloud. The BI team inside of IT is participating in that effort.
- The existing IT governance policy states that personal customer data and financial data must be hosted on assets owned directly by the company. This policy blocks cloud adoption for any mission-critical applications or protected data.
- IT investments are controlled largely by capital expense. Those investments are planned yearly and often include plans for ongoing maintenance, as well as established refresh cycles of three to five years depending on the datacenter.
- Most investments in technology that don't align to the annual plan are addressed by shadow IT efforts. Those efforts are usually managed by business units and funded through the business unit's operating expenses.

## Future state

The following changes are anticipated over the next several years:

- The CIO is leading an effort to modernize the policy on personal and financial data to support future goals. Two members of the IT governance team have visibility into this effort.
- The CIO wants to use the cloud migration as a forcing function to improve consistency and stability across business units and geographies. The future state must respect any external compliance requirements that would require deviation from standard approaches by specific IT teams.
- If the early experiments in application development and BI show leading indicators of success, they would each like to release small-scale production solutions to the cloud in the next 24 months.
- The CIO and CFO have assigned an architect and the vice president of infrastructure to create a cost analysis and feasibility study. These efforts will determine whether the company can and should move 5,000 assets to the cloud over the next 36 months. A successful migration would allow the CIO to eliminate two datacenters, reducing costs by over \$100m USD during the five-year plan. If three to four datacenters can experience similar results, the budget will be back in the black, giving the CIO budget to support more innovative initiatives.



- Along with this cost savings, the company plans to change the management of some IT investments by repositioning the committed capital expense as an operating expense within IT. This change will provide greater cost control that IT can use to accelerate other planned efforts.

## Next steps

The company has developed a corporate policy to shape the governance implementation. The corporate policy drives many of the technical decisions.

[Review the initial corporate policy](#)

# Governance guide for complex enterprises: Initial corporate policy behind the governance strategy

11/9/2020 • 5 minutes to read • [Edit Online](#)

The following corporate policy defines the initial governance position that's the starting point for this guide. This article defines early-stage risks, initial policy statements, and early processes to enforce policy statements.

## NOTE

The corporate policy is not a technical document, but it drives many technical decisions. The governance MVP described in the [overview](#) ultimately derives from this policy. Before implementing a governance MVP, your organization should develop a corporate policy based on your own objectives and business risks.

## Cloud governance team

The CIO recently held a meeting with the IT governance team to understand the history of the personal data and mission-critical policies and review the effect of changing those policies. The CIO also discussed the overall potential of the cloud for IT and the company.

After the meeting, two members of the IT governance team requested permission to research and support the cloud planning efforts. Recognizing the need for governance and an opportunity to limit shadow IT, the director of IT governance supported this idea. With that, the cloud governance team was born. Over the next several months, they will inherit the cleanup of many mistakes made during exploration in the cloud from a governance perspective. This will earn them the moniker of *cloud custodians*. In later iterations, this guide will show how their roles change over time.

## Objective

The initial objective is to establish a foundation for governance agility. An effective Governance MVP allows the governance team to stay ahead of cloud adoption and implement guardrails as the adoption plan changes.

## Business risks

The company is at an early stage of cloud adoption, experimenting and building proofs of concept. Risks are now relatively low, but future risks are likely to have a significant impact. There is little definition around the final state of the technical solutions to be deployed to the cloud. In addition, the cloud readiness of IT employees is low. A foundation for cloud adoption will help the team safely learn and grow.

**Future-proofing:** There is a risk of not empowering growth, but also a risk of not providing the right protections against future risks.

An agile yet robust governance approach is needed to support the board's vision for corporate and technical growth. Failure to implement such a strategy will slow technical growth, potentially risking current and future market share growth. The impact of such a business risk is unquestionably high. However, the role IT will play in those potential future states is unknown, making the risk associated with current IT efforts relatively high. That said, until more concrete plans are aligned, the business has a high tolerance for risk.

This business risk can be broken down tactically into several technical risks:

- Well-intended corporate policies could slow transformation efforts or break critical business processes, if not

considered within a structured approval flow.

- The application of governance to deployed assets could be difficult and costly.
- Governance may not be properly applied across an application or workload, creating gaps in security.
- With so many teams working in the cloud, there is a risk of inconsistency.
- Costs may not properly align to business units, teams, or other budgetary management units.
- The use of multiple identities to manage various deployments could lead to security issues.
- Despite current policies, there is a risk that protected data could be mistakenly deployed to the cloud.

## Tolerance indicators

The current risk tolerance is high and the appetite for investing in cloud governance is low. As such, the tolerance indicators act as an early warning system to trigger the investment of time and energy. If the following indicators are observed, it would be wise to advance the governance strategy.

- **Cost Management discipline:** Scale of deployment exceeds 1,000 assets to the cloud, or monthly spending exceeds \$10,000 USD per month.
- **Identity Baseline discipline:** Inclusion of applications with legacy or third-party multi-factor authentication requirements.
- **Security Baseline discipline:** Inclusion of protected data in defined cloud adoption plans.
- **Resource Consistency discipline:** Inclusion of any mission-critical applications in defined cloud adoption plans.

## Policy statements

The following policy statements establish the requirements needed to remediate the defined risks. These policies define the functional requirements for the governance MVP. Each will be represented in the implementation of the governance MVP.

Cost Management:

- For tracking purposes, all assets must be assigned to an application owner within one of the core business functions.
- When cost concerns arise, additional governance requirements will be established with the finance team.

Security Baseline:

- Any asset deployed to the cloud must have an approved data classification.
- No assets identified with a protected level of data may be deployed to the cloud, until sufficient requirements for security and governance can be approved and implemented.
- Until minimum network security requirements can be validated and governed, cloud environments are seen as perimeter networks and should meet similar connection requirements to other datacenters or internal networks.

Resource Consistency:

- Because no mission-critical workloads are deployed at this stage, there are no SLA, performance, or BCDR requirements to be governed.
- When mission-critical workloads are deployed, additional governance requirements will be established with IT operations.

Identity Baseline:

- All assets deployed to the cloud should be controlled using identities and roles approved by current governance policies.

- All groups in the on-premises Active Directory infrastructure that have elevated privileges should be mapped to an approved RBAC role.

Deployment Acceleration:

- All assets must be grouped and tagged according to defined grouping and tagging strategies.
- All assets must use an approved deployment model.
- Once a governance foundation has been established for a cloud provider, any deployment tooling must be compatible with the tools defined by the governance team.

## Processes

No budget has been allocated for ongoing monitoring and enforcement of these governance policies. Because of that, the cloud governance team has improvised ways to monitor adherence to policy statements.

- **Education:** The cloud governance team is investing time to educate the cloud adoption teams on the governance guides that support these policies.
- **Deployment reviews:** Before deploying any asset, the cloud governance team will review the governance guide with the cloud adoption teams.

## Next steps

This corporate policy prepares the cloud governance team to implement the governance MVP as the foundation for adoption. The next step is to implement this MVP.

[Best practices explained](#)

# Governance guide for complex enterprises: Best practices explained

11/9/2020 • 11 minutes to read • [Edit Online](#)

The governance guide begins with a set of initial [corporate policies](#). These policies are used to establish a minimum viable product (MVP) for governance that reflects [best practices](#).

In this article, we discuss the high-level strategies that are required to create a governance MVP. The core of the governance MVP is the [Deployment Acceleration discipline](#). The tools and patterns applied at this stage will enable the incremental improvements needed to expand governance in the future.

## Governance MVP (initial governance foundation)

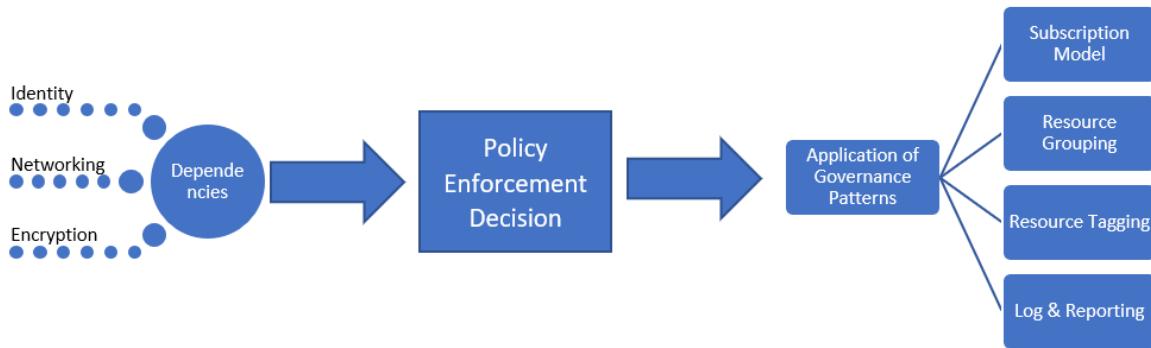
Rapid adoption of governance and corporate policy is achievable, thanks to a few simple principles and cloud-based governance tooling. These are the first of the three governance disciplines to approach in any governance process. Each discipline will be explained further on in this article.

To establish the starting point, this article discusses the high-level strategies behind the Security Baseline, Identity Baseline, and Deployment Acceleration disciplines that are required to create a governance MVP. The MVP serves as the foundation for all cloud adoption.



## Implementation process

The implementation of the governance MVP has dependencies on identity, security, and networking. Once the dependencies are resolved, the cloud governance team will decide a few aspects of governance. The decisions from the cloud governance team and from supporting teams will be implemented through a single package of enforcement assets.



This implementation can also be described using a simple checklist:

1. Solicit decisions regarding core dependencies: identity, network, and encryption.
2. Determine the pattern to be used during corporate policy enforcement.
3. Determine the appropriate governance patterns for resource consistency, resource tagging, and logging and reporting.
4. Implement the governance tools aligned to the chosen policy enforcement pattern to apply the dependent decisions and governance decisions.

## Dependent decisions

The following decisions come from teams outside of the cloud governance team. The implementation of each will come from those same teams. However, the cloud governance team is responsible for implementing a solution to validate that those implementations are consistently applied.

### Identity Baseline

Identity Baseline is the fundamental starting point for all governance. Before attempting to apply governance, identity must be established. The established identity strategy will then be enforced by the governance solutions. In this governance guide, the Identity Management team implements the [Directory Synchronization](#) pattern:

- RBAC will be provided by Azure Active Directory (Azure AD), using the directory synchronization or "Same Sign-On" that was implemented during company's migration to Microsoft 365. For implementation guidance, see [Reference Architecture for Azure AD Integration](#).
- The Azure AD tenant will also govern authentication and access for assets deployed to Azure.

In the governance MVP, the governance team will enforce application of the replicated tenant through subscription governance tooling, discussed later in this article. In future iterations, the governance team could also enforce rich tooling in Azure AD to extend this capability.

### Security Baseline: Networking

Software Defined Network is an important initial aspect of the Security Baseline. Establishing the governance MVP depends on early decisions from the Security Management team to define how networks can be safely configured.

Given the lack of requirements, IT security is playing it safe and requires a [Cloud DMZ](#) pattern. That means governance of the Azure deployments themselves will be very light.

- Azure subscriptions may connect to an existing datacenter via VPN, but must follow all existing on-premises IT governance policies regarding connection of a perimeter network to protected resources. For implementation guidance regarding VPN connectivity, see [On-premises network connected to Azure using a VPN gateway](#).
- Decisions regarding subnet, firewall, and routing are currently being deferred to each application/workload lead.
- Additional analysis is required before releasing of any protected data or mission-critical workloads.

In this pattern, cloud networks can only connect to on-premises resources over an existing VPN that is compatible

with Azure. Traffic over that connection will be treated like any traffic coming from a perimeter network. Additional considerations may be required on the on-premises edge device to securely handle traffic from Azure.

The cloud governance team has proactively invited members of the networking and IT security teams to regular meetings, in order to stay ahead of networking demands and risks.

### **Security Baseline: Encryption**

Encryption is another fundamental decision within the Security Baseline discipline. Because the company currently does not yet store any protected data in the cloud, the Security Team has decided on a less aggressive pattern for encryption. At this point, a [cloud-native pattern for encryption](#) is suggested but not required of any development team.

- No governance requirements have been set regarding the use of encryption, because the current corporate policy does not permit mission-critical or protected data in the cloud.
- Additional analysis will be required before releasing any protected data or mission-critical workloads.

## **Policy enforcement**

The first decision to make regarding Deployment Acceleration is the pattern for enforcement. In this narrative, the governance team decided to implement the [Automated Enforcement](#) pattern.

- Azure Security Center will be made available to the security and identity teams to monitor security risks. Both teams are also likely to use Security Center to identify new risks and improve corporate policy.
- RBAC is required in all subscriptions to govern authentication enforcement.
- Azure Policy will be published to each management group and applied to all subscriptions. However, the level of policies being enforced will be very limited in this initial Governance MVP.
- Although Azure management groups are being used, a relatively simple hierarchy is expected.
- Azure Blueprints will be used to deploy and update subscriptions by applying RBAC requirements, Resource Manager Templates, and Azure Policy across management groups.

## **Apply the dependent patterns**

The following decisions represent the patterns to be enforced through the policy enforcement strategy above:

**Identity Baseline.** Azure Blueprints will set RBAC requirements at a subscription level to ensure that consistent identity is configured for all subscriptions.

**Security Baseline: Networking.** The cloud governance team maintains a Resource Manager template for establishing a VPN gateway between Azure and the on-premises VPN device. When an application team requires a VPN connection, the cloud governance team will apply the gateway Resource Manager template via Azure Blueprints.

**Security Baseline: Encryption.** At this point, no policy enforcement is required in this area. This will be revisited during later iterations.

## **Application of governance-defined patterns**

The cloud governance team will be responsible for the following decisions and implementations. Many will require inputs from other teams, but the cloud governance team is likely to own both the decision and implementation. The following sections outline the decisions made for this use case and details of each decision.

### **Subscription design**

The decision on what subscription design to use determines how Azure subscriptions get structured and how Azure management groups will be used to efficiently manage access, policies, and compliance of these subscription. In this narrative, the governance team has chosen a [mixed subscription strategy](#).

- As new requests for Azure resources arise, a *department* should be established for each major business unit in each operating geography. Within each of the departments, *subscriptions* should be created for each application archetype.
  - An application archetype is a means of grouping applications with similar needs. Common examples include:
    - Applications with protected data, governed applications (such as HIPAA or FedRAMP).
    - Low-risk applications.
    - Applications with on-premises dependencies.
    - SAP or other mainframe applications in Azure.
    - Applications that extend on-premises SAP or mainframe applications.
- Each organization has unique needs based on data classifications and the types of applications that support the business. Dependency mapping of the digital estate can help define the application archetypes in an organization.
- A common naming convention should be adopted as part of the subscription design, based on the above.

### **Resource consistency**

Resource consistency decisions determine the tools, processes, and effort required to ensure Azure resources are deployed, configured, and managed consistently within a subscription. In this narrative, [deployment consistency](#) has been chosen as the primary resource consistency pattern.

- Resource groups are created for applications using the lifecycle approach. Everything that is created, maintained, and retired together should reside a single resource group. For more information, see the [resource consistency decision guide](#).
- Azure Policy should be applied to all subscriptions from the associated management group.
- As part of the deployment process, Azure resource consistency templates for the resource group should be stored in source control.
- Each resource group is associated with a specific workload or application based on the lifecycle approach described above.
- Azure management groups enable updating governance designs as corporate policy matures.
- Extensive implementation of Azure Policy could exceed the team's time commitments and may not provide a great deal of value at this time. A simple default policy should be created and applied to each management group to enforce the small number of current cloud governance policy statements. This policy will define the implementation of specific governance requirements. Those implementations can then be applied across all deployed assets.

#### **IMPORTANT**

Any time a resource in a resource group no longer shares the same lifecycle, it should be moved to another resource group. Examples include common databases and networking components. While they may serve the application being developed, they may also serve other purposes and should therefore exist in other resource groups.

### **Resource tagging**

Resource tagging decisions determine how metadata is applied to Azure resources within a subscription to support operations, management, and accounting purposes. In this narrative, the [accounting](#) pattern has been chosen as the default model for resource tagging.

- Deployed assets should be tagged with values for:
  - Department or billing unit
  - Geography
  - Data classification

- Criticality
- SLA
- Environment
- Application archetype
- Application
- Application owner
- These values, along with the Azure management group and subscription associated with a deployed asset, will drive governance, operations, and security decisions.

## **Logging and reporting**

Logging and reporting decisions determine how your store log data and how the monitoring and reporting tools that keep IT staff informed on operational health are structured. In this narrative a [hybrid monitoring](#) pattern for logging and reporting is suggested, but not required of any development team at this point.

- No governance requirements are currently set regarding the specific data points to be collected for logging or reporting purposes. This is specific to this fictional narrative and should be considered an antipattern. Logging standards should be determined and enforced as soon as possible.
- Additional analysis is required before the release of any protected data or mission-critical workloads.
- Before supporting protected data or mission-critical workloads, the existing on-premises operational monitoring solution must be granted access to the workspace used for logging. Applications are required to meet security and logging requirements associated with the use of that tenant, if the application is to be supported with a defined SLA.

## **Incremental of governance processes**

Some of the policy statements cannot or should not be controlled by automated tooling. Other policies will require periodic effort from IT security and on-premises identity baseline teams. The cloud governance team will need to oversee the following processes to implement the last eight policy statements:

**Corporate policy changes:** The cloud governance team will make changes to the governance MVP design to adopt the new policies. The value of the governance MVP is that it will allow for the automatic enforcement of the new policies.

**Adoption acceleration:** The cloud governance team has been reviewing deployment scripts across multiple teams. They've maintained a set of scripts that serve as deployment templates. Those templates can be used by the cloud adoption teams and DevOps teams to more quickly define deployments. Each script contains the requirements for enforcing governance policies, and additional effort from cloud adoption engineers is not needed. As the curators of these scripts, they can implement policy changes more quickly. Additionally, they're viewed as accelerators of adoption. This ensures consistent deployments without strictly enforcing adherence.

**Engineer training:** The cloud governance team offers bimonthly training sessions and has created two videos for engineers. Both resources help engineers get up to speed quickly on the governance culture and how deployments are performed. The team is adding training assets to demonstrate the difference between production and nonproduction deployments, which helps engineers understand how the new policies affect adoption. This ensures consistent deployments without strictly enforcing adherence.

**Deployment planning:** Before deploying any asset containing protected data, the cloud governance team will be responsible for reviewing deployment scripts to validate governance alignment. Existing teams with previously approved deployments will be audited using programmatic tooling.

**Monthly audit and reporting:** Each month, the cloud governance team runs an audit of all cloud deployments to validate continued alignment to policy. When deviations are discovered, they're documented and shared with the cloud adoption teams. When enforcement doesn't risk a business interruption or data leak, the policies are automatically enforced. At the end of the audit, the cloud governance team compiles a report for the cloud

strategy team and each cloud adoption team to communicate overall adherence to policy. The report is also stored for auditing and legal purposes.

**Quarterly policy review:** Each quarter, the cloud governance team and the cloud strategy team to review audit results and suggest changes to corporate policy. Many of those suggestions are the result of continuous improvements and the observation of usage patterns. Approved policy changes are integrated into governance tooling during subsequent audit cycles.

## Alternative patterns

If any of the patterns chosen in this governance guide don't align with the reader's requirements, alternatives to each pattern are available:

- [Encryption patterns](#)
- [Identity patterns](#)
- [Logging and reporting patterns](#)
- [Policy enforcement patterns](#)
- [Resource consistency patterns](#)
- [Resource tagging patterns](#)
- [Software Defined Networking patterns](#)
- [Subscription design patterns](#)

## Next steps

Once this guidance is implemented, each cloud adoption team can proceed with a solid governance foundation. At the same time, the cloud governance team will work to continually update the corporate policies and governance disciplines.

Both teams will use the tolerance indicators to identify the next set of improvements needed to continue supporting cloud adoption. The next step for this company is incremental improvement of their governance baseline to support applications with legacy or third-party multi-factor authentication requirements.

[Improve the Identity Baseline discipline](#)

# Governance guide for complex enterprises: Improve the Identity Baseline discipline

11/9/2020 • 4 minutes to read • [Edit Online](#)

This article advances the narrative by adding identity baseline controls to the governance MVP.

## Advancing the narrative

The business justification for the cloud migration of the two datacenters was approved by the CFO. During the technical feasibility study, several roadblocks were discovered:

- Protected data and mission-critical applications represent 25% of the workloads in the two datacenters. Neither can be eliminated until the current governance policies regarding sensitive personal data and mission-critical applications have been modernized.
- 7% of the assets in those datacenters are not cloud-compatible. They will be moved to an alternate datacenter before termination of the datacenter contract.
- 15% of the assets in the datacenter (750 virtual machines) have a dependency on legacy authentication or third-party multi-factor authentication.
- The VPN connection that connects existing datacenters and Azure does not offer sufficient data transmission speeds or latency to migrate the volume of assets within the two-year timeline to retire the datacenter.

The first two roadblocks are being managed in parallel. This article will address the resolution of the third and fourth roadblocks.

### Expand the cloud governance team

The cloud governance team is expanding. Given the need for additional support regarding identity management, a systems administrator from the identity baseline team now participates in a weekly meeting to keep the existing team members aware of changes.

### Changes in the current state

The IT team has approval to move forward with the plans of the CIO and CFO to retire two datacenters. The team is concerned that 750 (15%) of the assets in those datacenters will have to be moved somewhere other than the cloud.

### Incrementally improve the future state

The new future state plans require a more robust identity baseline solution to migrate the 750 virtual machines with legacy authentication requirements. Beyond these two datacenters, this challenge is expected to affect similar percentages of assets in other datacenters.

The future state now also requires a connection from the cloud provider to the company's MPLS/leased-line solution.

The changes to current and future state expose new risks that will require new policy statements.

## Changes in tangible risks

**Business interruption during migration.** Migration to the cloud creates a controlled, time-bound risk that can be managed. Moving aging hardware to another part of the world is much higher risk. A mitigation strategy is needed to avoid interruptions to business operations.

**Existing identity dependencies.** Dependencies on existing authentication and identity services may delay or prevent the migration of some workloads to the cloud. Failure to return the two datacenters on time will incur millions of dollars in datacenter lease fees.

This business risk can be expanded into a few technical risks:

- Legacy authentication might not be available in the cloud, limiting deployment of some applications.
- The current third-party multi-factor authentication solution might not be available in the cloud, limiting deployment of some applications.
- Retooling or moving could create outages or add costs.
- The speed and stability of the VPN might impede migration.
- Traffic entering the cloud could cause security issues in other parts of the global network.

## Incremental improvement of the policy statements

The following changes to policy will help remediate the new risks and guide implementation.

- The chosen cloud provider must offer a means of authenticating via legacy methods.
- The chosen cloud provider must offer a means of authentication with the current third-party multi-factor authentication solution.
- A high-speed private connection should be established between the cloud provider and the company's telco provider, connecting the cloud provider to the global network of datacenters.
- Until sufficient security requirements are established, no inbound public traffic may access company assets hosted in the cloud. All ports are blocked from any source outside of the global WAN.

## Incremental improvement of best practices

The governance MVP design changes to include new Azure policies and an implementation of Active Directory on a virtual machine. Together, these two design changes fulfill the new corporate policy statements.

Here are the new best practices:

- **Secure hybrid virtual network blueprint:** The on-premises side of the hybrid network should be configured to allow communication between the following solution and the on-premises Active Directory servers. This best practice requires a perimeter network to enable Active Directory Domain Services across network boundaries.
- **Azure Resource Manager templates:**
  1. Define an NSG to block external traffic and allow internal traffic.
  2. Deploy two Active Directory virtual machines in a load-balanced pair based on a golden image. On first boot, that image runs a PowerShell script to join the domain and register with domain services. For more information, see [Extend Active Directory Domain Services \(AD DS\) to Azure](#).
- Azure Policy: apply the NSG to all resources.
- Azure Blueprints:
  1. Create a blueprint named `active-directory-virtual-machines` .
  2. Add each of the Active Directory templates and policies to the blueprint.
  3. Publish the blueprint to any applicable management group.
  4. Apply the blueprint to any subscription requiring legacy or third-party multi-factor authentication.
  5. The instance of Active Directory running in Azure can now be used as an extension of the on-premises Active Directory solution, allowing it to integrate with the existing multi-factor authentication tool and provide claims-based authentication, both through existing Active Directory functionality.

## Conclusion

Adding these changes to the governance MVP helps remediate many of the risks in this article, allowing each cloud adoption team to quickly move past this roadblock.

## Next steps

As cloud adoption continues and delivers additional business value, risks and cloud governance needs will also change. The following are a few changes that may occur. For this fictional company, the next trigger is the inclusion of protected data in the cloud adoption plan. This change requires additional security controls.

[Improve the Security Baseline discipline](#)

# Governance guide for complex enterprises: Improve the Security Baseline discipline

11/9/2020 • 13 minutes to read • [Edit Online](#)

This article advances the narrative by adding security controls that support moving protected data to the cloud.

## Advancing the narrative

The CIO has spent months collaborating with colleagues and the company's legal staff. A management consultant with expertise in cybersecurity was engaged to help the existing IT security and IT governance teams draft a new policy regarding protected data. The group was able to foster board support to replace the existing policy, allowing sensitive personal and financial data to be hosted by approved cloud providers. This required adopting a set of security requirements and a governance process to verify and document adherence to those policies.

For the past 12 months, the cloud adoption teams have cleared most of the 5,000 assets from the two datacenters to be retired. The 350 incompatible assets were moved to an alternate datacenter. Only the 1,250 virtual machines that contain protected data remain.

### Changes in the cloud governance team

The cloud governance team continues to change along with the narrative. The two founding members of the team are now among the most respected cloud architects in the company. The collection of configuration scripts has grown as new teams tackle innovative new deployments. The cloud governance team has also grown. Most recently, members of the IT operations team have joined cloud governance team activities to prepare for cloud operations. The cloud architects who helped foster this community are seen both as cloud guardians and cloud accelerators.

While the difference is subtle, it is an important distinction when building a governance-focused IT culture. A cloud custodian cleans up the messes made by innovative cloud architects, and the two roles have natural friction and opposing objectives. A cloud guardian helps keep the cloud safe, so other cloud architects can move more quickly with fewer messes. A cloud accelerator performs both functions but is also involved in the creation of templates to accelerate deployment and adoption, becoming an innovation accelerator as well as a defender of the Five Disciplines of Cloud Governance.

### Changes in the current state

In the previous phase of this narrative, the company had begun the process of retiring two datacenters. This ongoing effort includes migrating some applications with legacy authentication requirements, which required incremental improvements to the Identity Baseline discipline, described in the [previous article](#).

Since then, some things have changed that will affect governance:

- Thousands of IT and business assets have been deployed to the cloud.
- The application development team has implemented a continuous integration and continuous deployment (CI/CD) pipeline to deploy a cloud-native application with an improved user experience. That application doesn't interact with protected data yet, so it isn't production ready.
- The business intelligence team within IT actively curates data in the cloud from logistics, inventory, and third-party data. This data is being used to drive new predictions, which could shape business processes. Those predictions and insights are not actionable until customer and financial data can be integrated into the data platform.
- The IT team is making progress on the CIO and CFO plans to retire two datacenters. Almost 3,500 of the assets in the two datacenters have been retired or migrated.

- The policies regarding sensitive personal and financial data have been modernized. The new corporate policies are contingent on the implementation of related security and governance policies. Teams are still stalled.

### **Incrementally improve the future state**

- Early experiments from the application development and BI teams have shown potential improvements in customer experiences and data-driven decisions. Both teams would like to expand adoption of the cloud over the next 18 months by deploying those solutions to production.
- IT has developed a business justification to migrate five more datacenters to Azure, which will further decrease IT costs and provide greater business agility. While smaller in scale, the retirement of those datacenters is expected to double the total cost savings.
- Capital expense and operating expense budgets have approved to implement the required security and governance policies, tools, and processes. The expected cost savings from the datacenter retirement are more than enough to pay for this new initiative. IT and business leadership are confident this investment will accelerate the realization of returns in other areas. The grassroots cloud governance team became a recognized team with dedicated leadership and staffing.
- Collectively, the cloud adoption teams, the cloud governance team, the IT security team, and the IT governance team will implement security and governance requirements to allow cloud adoption teams to migrate protected data into the cloud.

## **Changes in tangible risks**

**Data breach:** There is an inherent increase in liabilities related to data breaches when adopting any new data platform. Technicians adopting cloud technologies have increased responsibilities to implement solutions that can decrease this risk. A robust security and governance strategy must be implemented to ensure those technicians fulfill those responsibilities.

This business risk can be expanded into several technical risks:

1. Mission-critical applications or protected data might be deployed unintentionally.
2. Protected data might be exposed during storage due to poor encryption decisions.
3. Unauthorized users might access protected data.
4. External intrusion could result in access to protected data.
5. External intrusion or denial of service attacks could cause a business interruption.
6. Organization or employment changes could allow for unauthorized access to protected data.
7. New exploits might create opportunities for intrusion or unauthorized access.
8. Inconsistent deployment processes might result in security gaps that could lead to data leaks or interruptions.
9. Configuration drift or missed patches might result in unintended security gaps that could lead to data leaks or interruptions.
10. Disparate edge devices might increase network operations costs.
11. Disparate device configurations might lead to oversights in configuration and compromises in security.
12. The cybersecurity team insists there is a risk of vendor lock-in from generating encryption keys on a single cloud provider's platform. While this claim is unsubstantiated, it was accepted by the team for the time being.

## **Incremental improvement of the policy statements**

The following changes to policy will help remediate the new risks and guide implementation. The list looks long, but the adoption of these policies may be easier than it would appear.

1. All deployed assets must be categorized by criticality and data classification. Classifications are to be reviewed by the cloud governance team and the application before deployment to the cloud.
2. Applications that store or access protected data are to be managed differently than those that don't. At a minimum, they should be segmented to avoid unintended access of protected data.

3. All protected data must be encrypted when at rest.
4. Elevated permissions in any segment containing protected data should be an exception. Any such exceptions will be recorded with the cloud governance team and audited regularly.
5. Network subnets containing protected data must be isolated from any other subnets. Network traffic between protected data subnets will be audited regularly.
6. No subnet containing protected data can be directly accessed over the public internet or across datacenters. Access to these subnets must be routed through intermediate subnets. All access into these subnets must come through a firewall solution that can perform packet scanning and blocking functions.
7. Governance tooling must audit and enforce network configuration requirements defined by the security management team.
8. Governance tooling must limit VM deployment to approved images only.
9. Whenever possible, node configuration management should apply policy requirements to the configuration of any guest operating system. Node configuration management should respect the existing investment in group policy objects (GPO) for resource configuration.
10. Governance tooling will audit that automatic updates are enabled on all deployed assets. When possible, automatic updates will be enforced. When not enforced by tooling, node-level violations must be reviewed with operational management teams and remediated in accordance with operations policies. Assets that are not automatically updated must be included in processes owned by IT operations.
11. Creation of new subscriptions or management groups for any mission-critical applications or protected data requires a review from the cloud governance team to ensure proper blueprint assignment.
12. A least-privilege access model will be applied to any subscription that contains mission-critical applications or protected data.
13. The cloud vendor must be capable of integrating encryption keys managed by the existing on-premises solution.
14. The cloud vendor must be capable of supporting the existing edge device solution and any required configurations to protect any publicly exposed network boundary.
15. The cloud vendor must be capable of supporting a shared connection to the global WAN, with data transmission routed through the existing edge device solution.
16. Trends and exploits that could affect cloud deployments should be reviewed regularly by the security team to provide updates to Security Baseline tools used in the cloud.
17. Deployment tooling must be approved by the cloud governance team to ensure ongoing governance of deployed assets.
18. Deployment scripts must be maintained in a central repository accessible by the cloud governance team for periodic review and auditing.
19. Governance processes must include audits at the point of deployment and at regular cycles to ensure consistency across all assets.
20. Deployment of any applications that require customer authentication must use an approved identity provider that is compatible with the primary identity provider for internal users.
21. Cloud governance processes must include quarterly reviews with identity baseline teams to identify malicious actors or usage patterns that should be prevented by cloud asset configuration.

## Incremental improvement of best practices

This section modifies the governance MVP design to include new Azure policies and an implementation of Azure Cost Management + Billing. Together, these two design changes will fulfill the new corporate policy statements.

The new best practices fall into two categories: corporate IT (hub) and cloud adoption (spoke).

**Establishing a corporate IT hub and spoke subscription to centralize the security baseline:** In this best practice, the existing governance capacity is wrapped by a [hub and spoke topology with shared services](#), with a few key additions from the cloud governance team.

1. Azure DevOps repository. Create a repository in Azure DevOps to store and version all relevant Azure Resource

Manager templates and scripted configurations.

2. Hub and spoke template:

- a. The guidance in the [hub and spoke topology with shared services](#) reference architecture can be used to generate Resource Manager templates for the assets required in a corporate IT hub.
  - b. Using those templates, this structure can be made repeatable, as part of a central governance strategy.
  - c. In addition to the current reference architecture, a network security group template should be created to capture any port blocking or allow-listing requirements for the virtual network to host the firewall. This network security group differs from prior groups, because it will be the first network security group to allow public traffic into a virtual network.
3. Create Azure policies. Create a policy named `hub NSG enforcement` to enforce the configuration of the network security group assigned to any virtual network created in this subscription. Apply the built-in policies for guest configuration as follows:
- a. Audit that Windows web servers are using secure communication protocols.
  - b. Audit that password security settings are set correctly inside Linux and Windows machines.
4. Create the corporate IT blueprint.
- a. Create an Azure blueprint named `corporate-it-subscription`.
  - b. Add the hub and spoke templates and `hub NSG enforcement` policy.
5. Expanding on initial management group hierarchy.
- a. For each management group that has requested support for protected data, the `corporate-it-subscription-blueprint` blueprint provides an accelerated hub solution.
  - b. Because management groups in this fictional example include a regional hierarchy in addition to a business unit hierarchy, this blueprint will be deployed in each region.
  - c. For each region in the management group hierarchy, create a subscription named `corporate IT subscription`.
  - d. Apply the `corporate-it-subscription-blueprint` blueprint to each regional instance.
  - e. This will establish a hub for each business unit in each region. Note: further cost savings could be achieved by sharing hubs across business units in each region.
6. Integrate group policy objects (GPO) through Desired State Configuration (DSC):
- a. Convert GPO to DSC. The [Microsoft baseline management project](#) in GitHub can accelerate this effort. Be sure to store DSC in the repository in parallel with Resource Manager templates.
  - b. Deploy Azure Automation state configuration to any instances of the corporate IT subscription. Azure Automation can be used to apply DSC to VMs deployed in supported subscriptions within the management group.
  - c. The current roadmap aims to enable custom guest configuration policies. When that feature is released, the use of Azure Automation in this best practice will no longer be required.

**Applying additional governance to a cloud adoption subscription (spoke):** Building on the `corporate IT subscription`, minor changes to the governance MVP applied to each subscription dedicated to the support of application archetypes can produce rapid improvement.

In prior iterative changes to the best practice, we defined network security groups to block public traffic and allow internal traffic. Additionally, the Azure blueprint temporarily created DMZ and Active Directory capabilities. In this iteration, we will tweak those assets a bit, creating a new version of the Azure blueprint.

1. Network peering template. This template will peer the virtual network in each subscription with the hub virtual network in the corporate IT subscription.
  - a. The reference architecture from the prior section, [hub and spoke topology with shared services](#), generated a Resource Manager template for enabling virtual network peering.
  - b. That template can be used as a guide to modify the DMZ template from the prior governance iteration.
  - c. We are now adding virtual network peering to the DMZ virtual network that was previously connected

- to the local edge device over VPN.
- d. The VPN should also be removed from this template as well to ensure no traffic is routed directly to the on-premises datacenter, without passing through the corporate IT subscription and firewall solution. You could also set this VPN as a failover circuit in the event of an ExpressRoute circuit outage.
  - e. Additional [network configuration](#) is required by Azure Automation to apply DSC to hosted VMs.
2. Modify the network security group. Block all public **and** direct on-premises traffic in the network security group. The only inbound traffic should be coming through the virtual network peer in the corporate IT subscription.
- a. In the prior iteration, a network security group was created blocking all public traffic and allowing all internal traffic. Now we want to shift this network security group a bit.
  - b. The new network security group configuration should block all public traffic, along with all traffic from the local datacenter.
  - c. Traffic entering this virtual network should only come from the virtual network on the other side of the virtual network peer.
3. Azure Security Center implementation:
- a. Configure Azure Security Center for any management group that contains protected data classifications.
  - b. Set automatic provisioning to on by default to ensure patching compliance.
  - c. Establish OS security configurations. IT security to define the configuration.
  - d. Support IT security in the initial use of Azure Security Center. Transition use of Security Center to IT security, but maintain access for governance continuous improvement purposes.
  - e. Create a Resource Manager template reflecting the changes required for Azure Security Center configuration within a subscription.
4. Update Azure Policy for all subscriptions.
- a. Audit and enforce criticality and data classification across all management groups and subscriptions to identify any subscriptions with protected data classifications.
  - b. Audit and enforce use of approved OS images only.
  - c. Audit and enforce guest configurations based on security requirements for each node.
5. Update Azure Policy for all subscriptions that contains protected data classifications.
- a. Audit and enforce use of standard roles only.
  - b. Audit and enforce application of encryption for all storage accounts and files at rest on individual nodes.
  - c. Audit and enforce the application of the new version of the DMZ network security group.
  - d. Audit and enforce use of approved network subnet and virtual network per network interface.
  - e. Audit and enforce the limitation of user-defined routing tables.
6. Azure blueprint:
- a. Create an Azure blueprint named `protected-data`.
  - b. Add the virtual network peer, network security group, and Azure Security Center templates to the blueprint.
  - c. Ensure the template for Active Directory from the previous iteration is **not** included in the blueprint. Any dependencies on Active Directory will be provided by the corporate IT subscription.
  - d. Terminate any existing Active Directory VMs deployed in the previous iteration.
  - e. Add the new policies for protected data subscriptions.
  - f. Publish the blueprint to any management group that will host protected data.
  - g. Apply the new blueprint to each affected subscription along with existing blueprints.

## Conclusion

Adding these processes and changes to the governance MVP helps remediate many of the risks associated with security governance. Together, they add the network, identity, and security monitoring tools needed to protect data.

## Next steps

As cloud adoption continues and delivers additional business value, risks and cloud governance needs also change. For the fictional company in this guide, the next step is to support mission-critical workloads. This is the point when resource consistency controls are needed.

[Improve the Resource Consistency discipline](#)

# Governance guide for complex enterprises: Improve the Resource Consistency discipline

11/9/2020 • 6 minutes to read • [Edit Online](#)

This article advances the narrative by adding resource consistency controls to the governance MVP to support mission-critical applications.

## Advancing the narrative

The cloud adoption teams have met all requirements to move protected data. With those applications come SLA commitments to the business and need for support from IT operations. Right behind the team migrating the two datacenters, multiple application development and BI teams are ready to begin launching new solutions into production. IT operations is new to cloud operations and needs to quickly integrate existing operational processes.

### Changes in the current state

- IT is actively moving production workloads with protected data into Azure. Some low-priority workloads are serving production traffic. More can be cut over as soon as IT operations signs off on readiness to support the workloads.
- The application development teams are ready for production traffic.
- The BI team is ready to integrate predictions and insights into the systems that run operations for the three business units.

### Incrementally improve the future state

- IT operations is new to cloud operations and needs to quickly integrate existing operational processes.
- The changes to current and future state expose new risks that will require new policy statements.

## Changes in tangible risks

**Business interruption:** There is an inherent risk of any new platform causing interruptions to mission-critical business processes. The IT operations team and the teams executing on various cloud adoptions are relatively inexperienced with cloud operations. This increases the risk of interruption and must be remediated and governed.

This business risk can be expanded into several technical risks:

1. Misaligned operational processes might lead to outages that can't be detected or mitigated quickly.
2. External intrusion or denial of service attacks might cause a business interruption.
3. Mission-critical assets might not be properly discovered and therefore not properly operated.
4. Undiscovered or mislabeled assets might not be supported by existing operational management processes.
5. Configuration of deployed assets might not meet performance expectations.
6. Logging might not be properly recorded and centralized to allow for remediation of performance issues.
7. Recovery policies may fail or take longer than expected.
8. Inconsistent deployment processes might result in security gaps that could lead to data leaks or interruptions.
9. Configuration drift or missed patches might result in unintended security gaps that could lead to data leaks or interruptions.
10. Configuration might not enforce the requirements of defined SLAs or committed recovery requirements.
11. Deployed operating systems or applications might not meet OS and application hardening requirements.
12. There is a risk of inconsistency due to multiple teams working in the cloud.

## Incremental improvement of the policy statements

The following changes to policy will help remediate the new risks and guide implementation. The list looks long, but the adoption of these policies may be easier than it would appear.

1. All deployed assets must be categorized by criticality and data classification. Classifications are to be reviewed by the cloud governance team and the application owner before deployment to the cloud.
2. Subnets containing mission-critical applications must be protected by a firewall solution capable of detecting intrusions and responding to attacks.
3. Governance tooling must audit and enforce network configuration requirements defined by the security baseline team.
4. Governance tooling must validate that all assets related to mission-critical applications or protected data are included in monitoring for resource depletion and optimization.
5. Governance tooling must validate that the appropriate level of logging data is being collected for all mission-critical applications or protected data.
6. Governance process must validate that backup, recovery, and SLA adherence are properly implemented for mission-critical applications and protected data.
7. Governance tooling must limit virtual machine deployment to approved images only.
8. Governance tooling must enforce that automatic updates are **prevented** on all deployed assets that support mission-critical applications. Violations must be reviewed with operational management teams and remediated in accordance with operations policies. Assets that are not automatically updated must be included in processes owned by IT operations to quickly and effectively update those servers.
9. Governance tooling must validate tagging related to cost, criticality, SLA, application, and data classification. All values must align to predefined values managed by the cloud governance team.
10. Governance processes must include audits at the point of deployment and at regular cycles to ensure consistency across all assets.
11. Trends and exploits that could affect cloud deployments should be reviewed regularly by the security team to provide updates to Security Baseline tools used in the cloud.
12. Before release into production, all mission-critical applications and protected data must be added to the designated operational monitoring solution. Assets that cannot be discovered by the chosen IT operations tooling cannot be released for production use. Any changes required to make the assets discoverable must be made to the relevant deployment processes to ensure assets will be discoverable in future deployments.
13. When discovered, asset sizing is to be validated by operational management teams to validate that the asset meets performance requirements.
14. Deployment tooling must be approved by the cloud governance team to ensure ongoing governance of deployed assets.
15. Deployment scripts must be maintained in central repository accessible by the cloud governance team for periodic review and auditing.
16. Governance review processes must validate that deployed assets are properly configured in alignment with SLA and recovery requirements.

## Incremental improvement of best practices

This section of the article will improve the governance MVP design to include new Azure policies and an implementation of Azure Cost Management + Billing. Together, these two design changes will fulfill the new corporate policy statements.

Following the experience of this fictional example, it is assumed that the protected data changes have already occurred. Building on that best practice, the following will add operational monitoring requirements, readying a subscription for mission-critical applications.

**Corporate IT subscription:** Add the following to the corporate IT subscription, which acts as a hub.

1. As an external dependency, the cloud operations team will need to define operational monitoring tooling, business continuity and disaster recovery (BCDR) tooling, and automated remediation tooling. The cloud governance team can then support necessary discovery processes.
  - a. In this use case, the cloud operations team chose Azure Monitor as the primary tool for monitoring mission-critical applications.
  - b. The team also chose Azure Site Recovery as the primary BCDR tooling.
2. Azure Site Recovery implementation.
  - a. Define and deploy Azure Site Recovery vault for backup and recovery processes.
  - b. Create an Azure resource management template for creation of a vault in each subscription.
3. Azure Monitor implementation.
  - a. Once a mission-critical subscription is identified, a Log Analytics workspace can be created.

**Individual cloud adoption subscription:** The following will ensure that each subscription is discoverable by the monitoring solution and ready to be included in BCDR practices.

1. Azure Policy for mission-critical nodes:
  - a. Audit and enforce use of standard roles only.
  - b. Audit and enforce application of encryption for all storage accounts.
  - c. Audit and enforce use of approved network subnet and virtual network per network interface.
  - d. Audit and enforce the limitation of user-defined routing tables.
  - e. Audit and enforce the deployment of Log Analytics agents for Windows and Linux virtual machines.
2. Azure Blueprints:
  - a. Create a blueprint named `mission-critical-workloads-and-protected-data`. This blueprint will apply assets in addition to the protected data blueprint.
  - b. Add the new Azure policies to the blueprint.
  - c. Apply the blueprint to any subscription that is expected to host a mission-critical application.

## Conclusion

Adding these processes and changes to the governance MVP helps remediate many of the risks associated with resource governance. Together, they add the recovery, sizing, and monitoring controls necessary to empower cloud-aware operations.

## Next steps

As cloud adoption grows and delivers additional business value, the risks and cloud governance needs will also change. For the fictional company in this guide, the next trigger is when the scale of deployment exceeds 1,000 assets to the cloud or monthly spending exceeds \$10,000 USD per month. At this point, the cloud governance team adds cost management controls.

[Improve the Cost Management discipline](#)

# Governance guide for complex enterprises: Improve the Cost Management discipline

11/9/2020 • 4 minutes to read • [Edit Online](#)

This article advances the narrative by adding cost controls to the minimum viable product (MVP) governance.

## Advancing the narrative

Adoption has grown beyond the tolerance indicator defined in the governance MVP. The increases in spending now justifies an investment of time from the cloud governance team to monitor and control spending patterns.

As a clear driver of innovation, IT is no longer seen primarily as a cost center. As the IT organization delivers more value, the CIO and CFO agree that the time is right to shift the role IT plays in the company. Among other changes, the CFO wants to test a direct pay approach to cloud accounting for the Canadian branch of one of the business units. One of the two retired datacenters was exclusively hosted assets for that business unit's Canadian operations. In this model, the business unit's Canadian subsidiary will be billed directly for the operating expenses related to the hosted assets. This model allows IT to focus less on managing someone else's spending and more on creating value. Before this transition can begin cost management tooling needs to be in place.

### Changes in the current state

In the previous phase of this narrative, the IT team was actively moving production workloads with protected data into Azure.

Since then, some things have changed that will affect governance:

- 5,000 assets have been removed from the two datacenters flagged for retirement. Procurement and IT security are now deprovisioning the remaining physical assets.
- The application development teams have implemented CI/CD pipelines to deploy some cloud-native applications, significantly affecting customer experiences.
- The BI team has created aggregation, curation, insight, and prediction processes driving tangible benefits for business operations. Those predictions are now empowering creative new products and services.

### Incrementally improve the future state

Cost monitoring and reporting should be added to the cloud solution. Reporting should tie direct operating expenses to the functions that are consuming the cloud costs. Additional reporting should allow IT to monitor spending and provide technical guidance on cost management. For the Canadian branch, the department will be billed directly.

## Changes in risk

**Budget control:** There is an inherent risk that self-service capabilities will result in excessive and unexpected costs on the new platform. Governance processes for monitoring costs and mitigating ongoing cost risks must be in place to ensure continued alignment with the planned budget.

This business risk can be expanded into a few technical risks:

- There is a risk of actual costs exceeding the plan.
- Business conditions change. When they do, there will be cases when a business function needs to consume more cloud services than expected, leading to spending anomalies. There is a risk that these additional costs will be considered overages as opposed to a required adjustment to the plan. If successful, the Canadian

experiment should help remediate this risk.

- There is a risk of systems being overprovisioned, resulting in excess spending.

## Changes to the policy statements

The following changes to policy will help remediate the new risks and guide implementation.

- All cloud costs should be monitored against plan on a weekly basis by the cloud governance team. Reporting on deviations between cloud costs and plan is to be shared with IT leadership and finance monthly. All cloud costs and plan updates should be reviewed with IT leadership and finance monthly.
- All costs must be allocated to a business function for accountability purposes.
- Cloud assets should be continually monitored for optimization opportunities.
- Cloud governance tooling must limit asset sizing options to an approved list of configurations. The tooling must ensure that all assets are discoverable and tracked by the cost monitoring solution.
- During deployment planning, any required cloud resources associated with the hosting of production workloads should be documented. This documentation will help refine budgets and prepare additional automation tools to prevent the use of more expensive options. During this process consideration should be given to different discounting tools offered by the cloud provider, such as Azure Reserved Virtual Machine Instances or license cost reductions.
- All application owners are required to attend trained on practices for optimizing workloads to better control cloud costs.

## Incremental improvement of best practices

This section of the article will improve the governance MVP design to include new Azure policies and an implementation of Azure Cost Management + Billing. Together, these two design changes will fulfill the new corporate policy statements.

1. Make changes in the Azure EA portal to bill the department administrator for the Canadian deployment.
2. Implement Azure Cost Management + Billing.
  - a. Establish the right level of access scope to align with the subscription pattern and resource grouping pattern. Assuming alignment with the governance MVP defined in prior articles, this would require **enrollment account scope** access for the cloud governance team executing on high-level reporting. Additional teams outside of governance, like the Canadian procurement team, will require **resource group scope** access.
  - b. Establish a budget in Azure Cost Management + Billing.
  - c. Review and act on initial recommendations. Create a recurring process to support the reporting process.
  - d. Configure and execute Azure Cost Management + Billing reporting, both initial and recurring.
3. Update Azure Policy.
  - a. Audit tagging, management group, subscription, and resource group values to identify any deviation.
  - b. Establish SKU size options to limit deployments to SKUs listed in deployment planning documentation.

## Conclusion

Adding the above processes and changes to the governance MVP helps remediate many of the risks associated with cost governance. Together, they create the visibility, accountability, and optimization needed to control costs.

## Next steps

As cloud adoption grows and delivers additional business value, risks and cloud governance needs will also change. For this fictional company, the next step is using this governance investment to manage multiple clouds.

Multicloud improvement

# Governance guide for complex enterprises: Multicloud improvement

11/9/2020 • 3 minutes to read • [Edit Online](#)

## Advancing the narrative

Microsoft recognizes that customers may adopt multiple clouds for specific purposes. The fictional company in this guide is no exception. In parallel with their Azure adoption journey, business success has led to the acquisition of a small but complementary business. That business is running all of their IT operations on a different cloud provider.

This article describes how things change when integrating the new organization. For purposes of the narrative, we assume this company has completed each of the governance iterations outlined in this governance guide.

### Changes in the current state

In the previous phase of this narrative, the company had begun to implement cost controls and cost monitoring, as cloud spending becomes part of the company's regular operating expenses.

Since then, some things have changed that will affect governance:

- Identity is controlled by an on-premises instance of Active Directory. Hybrid identity is facilitated through replication to Azure Active Directory.
- IT operations or cloud operations are largely managed by Azure Monitor and related automation capabilities.
- Business continuity and disaster recovery (BCDR) is controlled by Azure Recovery Services vaults.
- Azure Security Center is used to monitor security violations and attacks.
- Azure Security Center and Azure Monitor are both used to monitor governance of the cloud.
- Azure Blueprints, Azure Policy, and management groups are used to automate compliance to policy.

### Incrementally improve the future state

The goal is to integrate the acquisition company into existing operations wherever possible.

## Changes in tangible risks

**Business acquisition cost:** Acquisition of the new business is estimated to be profitable in approximately five years. Because of the slow rate of return, the board wants to control acquisition costs, as much as possible. There is a risk of cost control and technical integration conflicting with one another.

This business risk can be expanded into a few technical risks:

- There is a risk of cloud migration producing additional acquisition costs.
- There is also a risk of the new environment not being properly governed or resulting in policy violations.

## Incremental improvement of the policy statements

The following changes to policy will help remediate the new risks and guide implementation.

- All assets in a secondary cloud must be monitored through existing operational management and security monitoring tools.
- All organizational units must be integrated into the existing identity provider.
- The primary identity provider should govern authentication to assets in the secondary cloud.

## Incremental improvement of best practices

This section of the article improves the governance MVP design to include new Azure policies and an implementation of Azure Cost Management + Billing. Together, these two design changes will fulfill the new corporate policy statements.

1. Connect the networks. Executed by networking and IT security, supported by governance.
  - a. Adding a connection from the MPLS or leased-line provider to the new cloud will integrate networks.  
Adding routing tables and firewall configurations will control access and traffic between the environments.
2. Consolidate identity providers. Depending on the workloads being hosted in the secondary cloud, there are a variety of options to identity provider consolidation. The following are a few examples:
  - a. For applications that authenticate using OAuth 2, users in the Active Directory in the secondary cloud could simply be replicated to the existing Azure AD tenant.
  - b. On the other extreme, federation between the two on-premises identity providers, would allow users from the new Active Directory domains to be replicated to Azure.
3. Add assets to Azure Site Recovery.
  - a. Azure Site Recovery was built as a hybrid and multicloud tool from the beginning.
  - b. Virtual machines in the secondary cloud might be able to be protected by the same Azure Site Recovery processes used to protect on-premises assets.
4. Add assets to Azure Cost Management + Billing.
  - a. Azure Cost Management + Billing was built as a multicloud tool from the beginning.
  - b. Virtual machines in the secondary cloud might be compatible with Azure Cost Management + Billing for some cloud providers. Additional costs may apply.
5. Add assets to Azure Monitor.
  - a. Azure Monitor was built as a hybrid cloud tool from the beginning.
  - b. Virtual machines in the secondary cloud might be compatible with Azure Monitor agents, allowing them to be included in Azure Monitor for operational monitoring.
6. Governance enforcement tools.
  - a. Governance enforcement is cloud-specific.
  - b. The corporate policies established in the governance guide are not cloud-specific. While the implementation may vary from cloud to cloud, the policy statements can be applied to the secondary provider.

Multicloud adoption should be contained to where it is required based on technical needs or specific business requirements. As multicloud adoption grows, so does complexity and security risks.

## Next steps

In many large enterprises, the Five Disciplines of Cloud Governance can be blockers to adoption. The next article has some additional thoughts on making governance a team sport to help ensure long-term success in the cloud.

[Multiple layers of governance](#)

# Governance guide for complex enterprises: Multiple layers of governance

11/9/2020 • 3 minutes to read • [Edit Online](#)

When large enterprises require multiple layers of governance, there are greater levels of complexity that must be factored into the governance MVP and later governance improvements.

A few common examples of such complexities include:

- Distributed governance functions.
- Corporate IT supporting business unit IT organizations.
- Corporate IT supporting geographically distributed IT organizations.

This article explores some ways to navigate this type of complexity.

## Large enterprise governance is a team sport

Large established enterprises often have teams or employees who focus on the disciplines mentioned throughout this guide. This guide demonstrates one approach to making governance a team sport.

In many large enterprises, the Five Disciplines of Cloud Governance can be blockers to adoption. Developing cloud expertise in identity, security, operations, deployments, and configuration across an enterprise takes time.

Holistically implementing IT governance policy and IT security can slow innovation by months or even years.

Balancing the business need to innovate and the governance need to protect existing resources is delicate.

The inherent capabilities of the cloud can remove blockers to innovation but increase risks. In this governance guide, we showed how the example company created guardrails to manage the risks. Rather than tackling each of the disciplines required to protect the environment, the cloud governance team leads a risk-based approach to govern what could be deployed, while the other teams build the necessary cloud maturities. Most importantly, as each team reaches cloud maturity, governance applies their solutions holistically. As each team matures and adds to the overall solution, the cloud governance team can open stage gates, allowing additional innovation and adoption to thrive.

This model illustrates the growth of a partnership between the cloud governance team and existing enterprise teams (security, IT governance, networking, identity, and others). The guide starts with the governance MVP and grows to a holistic end state through governance iterations.

## Requirements to supporting such a team sport

The first requirement of a multilayer governance model is to understand of the governance hierarchy. Answering the following questions will help you to understand the general governance hierarchy:

- How is cloud accounting (billing for cloud services) allocated across business units?
- How are governance responsibilities allocated across corporate IT and each business unit?
- What types of environments do each of those units of IT manage?

## Central governance of a distributed governance hierarchy

Tools like management groups allow corporate IT to create a hierarchy structure that matches the governance hierarchy. Tools like Azure Blueprints can apply assets to different layers of that hierarchy. Azure Blueprints can be versioned and various versions can be applied to management groups, subscriptions, or resource groups. Each of

these concepts is described in more detail in the governance MVP.

The important aspect of each of these tools is the ability to apply multiple blueprints to a hierarchy. This allows governance to be a layered process. The following is one example of this hierarchical application of governance:

- **Corporate IT:** Corporate IT creates a set of standards and policies that apply to all cloud adoption. This is materialized in a *baseline* blueprint. Corporate IT then owns the management group hierarchy, ensuring that a version of the baseline is applied to all subscriptions in the hierarchy.
- **Regional or business unit IT:** Various IT teams can apply an additional layer of governance by creating their own blueprint. Those blueprints would create additive policies and standards. Once developed, corporate IT could apply those blueprints to the applicable nodes within the management group hierarchy.
- **Cloud adoption teams:** Detailed decisions and implementation about applications or workloads can be made by each cloud adoption team, within the context of governance requirements. The team can also request additional Azure resource consistency templates to accelerate adoption efforts.

The details regarding governance implementation at each level will require coordination between each team. The governance MVP and governance improvements outlined in this guide can aid in aligning that coordination.

# Evaluate corporate policy

11/9/2020 • 2 minutes to read • [Edit Online](#)

Any change to business processes or technology platforms introduces risk to the business. Cloud governance teams, whose members are sometimes known as cloud custodians, are tasked with mitigating these risks with minimal interruption to adoption or innovation efforts.

But cloud governance requires more than technical implementation. Subtle changes in the corporate narrative or corporate policies can affect adoption efforts significantly. Before implementation, it's important to look beyond IT while defining corporate policy.



Figure 1: Visual of corporate policy and the Five Disciplines of Cloud Governance.

## Define corporate policy

Defining corporate policy focuses on identifying and mitigating business risks regardless of the cloud platform. Healthy cloud governance strategy begins with sound corporate policy. The following three-step process guides the iterative development of such policies.

	<b>Business risk:</b> Investigate current cloud adoption plans and data classification to identify risks to the business. Work with the business to balance risk tolerance and mitigation costs.
	<b>Policy and compliance:</b> Evaluate risk tolerance to inform minimally invasive policies that govern cloud adoption and manage risks. In some industries, third-party compliance affects initial policy creation.
	<b>Processes:</b> The pace of adoption and innovation activities will naturally create policy violations. Executing relevant processes will aid in monitoring and enforcing adherence to policies.

## Next steps

Learn how to prepare your corporate policy for the cloud.

[Prepare your corporate policy for the cloud](#)

# Prepare corporate IT policy for the cloud

11/9/2020 • 4 minutes to read • [Edit Online](#)

Cloud governance is the product of an ongoing adoption effort over time, as a true lasting transformation doesn't happen overnight. Attempting to deliver complete cloud governance before addressing key corporate policy changes using a fast aggressive method seldom produces the desired results. Instead we recommend an incremental approach.

What is different about our Cloud Adoption Framework is the purchasing cycle and how it can enable authentic transformation. Since there is not a big capital expenditure acquisition requirement, engineers can begin experimentation and adoption sooner. In most corporate cultures, elimination of the capital expense barrier to adoption can lead to tighter feedback loops, organic growth, and incremental execution.

The shift to cloud adoption requires a shift in governance. In many organizations, corporate policy transformation allows for improved governance and higher rates of adherence through incremental policy changes and automated enforcement of those changes, powered by newly defined capabilities that you configure with your cloud service provider.

This article outlines key activities that can help you shape your corporate policies to enable an expanded governance model.

## Define corporate policy to mature cloud governance

In traditional governance and incremental governance, corporate policy creates the working definition of governance. Most IT governance actions seek to implement technology to monitor, enforce, operate, and automate those corporate policies. Cloud governance is built on similar concepts.

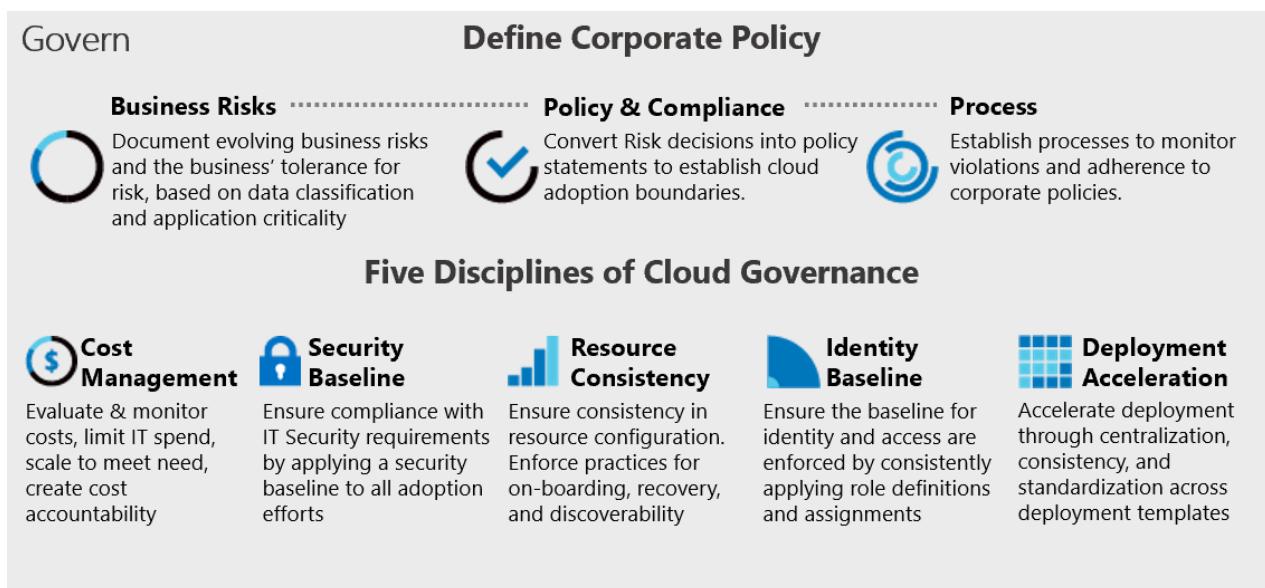


Figure 1: Corporate governance and governance disciplines.

The image above demonstrates the interactions between business risk, policy and compliance, and monitor and enforce to create a governance strategy. Followed by the Five Disciplines of Cloud Governance to realize your strategy.

## Review existing policies

In the image above, the governance strategy (risk, policy and compliance, monitor and enforce) starts with

recognizing business risks. Understanding how [business risk](#) changes in the cloud is the first step to creating a lasting cloud governance strategy. Working with your business units to gain an accurate [gauge of the business's tolerance for risk](#), helps you understand what level of risks need to be remediated. Your understanding of new risks and acceptable tolerance can fuel a [review of existing policies](#), in order to determine the required level of governance that is appropriate for your organization.

#### TIP

If your organization is governed by third-party compliance, one of the biggest business risks to consider may be a risk of adherence to [regulatory compliance](#). This risk often cannot be remediated, and instead may require a strict adherence. Be sure to understand your third-party compliance requirements before beginning a policy review.

## An incremental approach to cloud governance

An incremental approach to cloud governance assumes that it is unacceptable to exceed the [business's tolerance for risk](#). Instead, it assumes that the role of governance is to accelerate business change, help engineers understand architecture guidelines, and ensure that [business risks](#) are regularly communicated and remediated. Alternatively, the traditional role of governance can become a barrier to adoption by engineers or by the business as a whole.

With an incremental approach to cloud governance, there is sometimes a natural friction between teams building new business solutions and teams protecting the business from risks. In this model, those two teams can become peers working in increments or sprints. As peers, the cloud governance team and the cloud adoption teams begin to work together to expose, evaluate, and remediate business risks. This effort can create a natural means of reducing friction and building collaboration between teams.

## Minimum viable product (MVP) for policy

The first step in an emerging partnership between your cloud governance and adoption teams is an agreement regarding the policy MVP. Your MVP for cloud governance should acknowledge that business risks are small in the beginning, but will likely grow as your organization adopts more cloud services over time.

For example, the business risk is small for a business deploying five VMs that don't contain any high business impact (HBI) data. Later in the cloud adoption process, when the number reaches 1,000 VMs and the business is starting to move HBI data, the business risk grows.

Policy MVP attempts to define a required foundation for policies needed to deploy the first  $x$  VMs or the first  $x$  number of applications, where  $x$  is a small yet meaningful quantity of the units being adopted. This policy set requires few constraints, but would contain the foundational aspects needed to quickly grow from one incremental cloud adoption effort to the next. Through incremental policy development, this governance strategy would grow over time. Through slow subtle shifts, the policy MVP would grow into feature parity with the outputs of the policy review exercise.

## Incremental policy growth

Incremental policy growth is the key mechanism to growing policy and cloud governance over time. It is also the key requirement to adopting an incremental model to governance. For this model to work well, the governance team must be committed to an ongoing allocation of time at each sprint, in order to evaluate and implement changing governance disciplines.

**Sprint time requirements:** At the beginning of each iteration, each cloud adoption team creates a list of assets to be migrated or adopted in the current increment. The cloud governance team is expected to allow sufficient time to review the list, validate data classifications for assets, evaluate any new risks associated with each asset, update architecture guidelines, and educate the team on the changes. These commitments commonly require 10-

30 hours per sprint. It's also expected for this level of involvement to require at least one dedicated employee to manage governance in a large cloud adoption effort.

**Release time requirements:** At the beginning of each release, the cloud adoption teams and the cloud strategy team should prioritize a list of applications or workloads to be migrated in the current iteration, along with any business change activities. Those data points allow the cloud governance team to understand new business risks early. That allows time to align with the business and gauge the business's tolerance for risk.

## Next steps

Effective cloud governance strategy begins with understanding business risk.

[Understand business risk](#)

# Understand business risk during cloud migration

11/9/2020 • 4 minutes to read • [Edit Online](#)

An understanding of business risk is one of the most important elements of any cloud transformation. Risk drives policy, and it influences monitoring and enforcement requirements. Risk heavily influences how we manage the digital estate, on-premises or in the cloud.

## Relativity of risk

Risk is relative. A small company with a few IT assets, in a closed building has little risk. Add users and an internet connection with access to those assets, the risk is intensified. When that small company grows to Fortune 500 status, the risks are exponentially greater. As revenue, business process, employee counts, and IT assets accumulate, risks increase and coalesce. IT assets that aid in generating revenue are at tangible risk of stopping that revenue stream in the event of an outage. Every moment of downtime equates to losses. Likewise, as data accumulates, the risk of harming customers grows.

In the traditional on-premises world, IT governance teams focus on assessing risks, creating processes to manage those risks, and deploying systems to ensure remediation measures are successfully implemented. These efforts work to balance risks required to operate in a connected, modern business environment.

## Understand business risks in the cloud

During a transformation, the same relative risks exist.

- During early experimentation, a few assets are deployed with little to no relevant data. The risk is small.
- When the first workload is deployed, risk goes up a little. This risk is easily remediated by choosing an inherently low risk application with a small user base.
- As more workloads come online, risks change at each release. New applications go live and risks change.
- When a company brings the first 10 or 20 applications online, the risk profile is much different than when the 1000th application goes into production in the cloud.

The assets that accumulated in the traditional, on-premises estate likely accumulated over time. The maturity of the business and IT teams was likely growing in a similar fashion. That parallel growth can tend to create some unnecessary policy baggage.

During a cloud transformation, both the business and IT teams have an opportunity to reset those policies and build new with a matured mindset.

## What is a business risk MVP?

A *minimum viable product (MVP)* is commonly used to define the smallest unit of something that can produce tangible value. In a business risk MVP, the cloud governance team starts with the assumption that some assets will be deployed to a cloud environment at some point in time. It's unknown what those assets are at the time, and the team may be unsure what types of data will be stored on those assets.

When planning for business risk, the cloud governance team could build for the worst case scenario and map every possible policy to the cloud. Identifying all potential business risks for all cloud usage scenarios can take considerable time and effort, potentially delaying the implementation of governance to your cloud workloads. This is not recommended, but is an option.

Conversely, an MVP approach can allow the team to define an initial starting point and set of assumptions that

would be true for most/all assets. This business risk MVP will support initial small scale or test cloud deployments, and then be used as a base for gradually identifying and remediating new risks as business needs arise or additional workloads are added to your cloud environment. This process allows you to apply governance throughout the cloud adoption process.

The following are a few basic examples of business risks that can be included as part of an MVP:

- All assets are at risk of being deleted (through error, mistake or maintenance).
- All assets are at risk of generating too much spending.
- All assets could be compromised by weak passwords or insecure settings.
- Any asset with open ports exposed to the internet are at risk of compromise.

The above examples are meant to establish MVP business risks as a theory. The actual list will be unique to every environment.

Once the business risk MVP is established, they can be converted to [policies](#) to remediate each risk.

## Incremental risk mitigation

As your organization deploys more workloads to the cloud, development teams will make use of increasing amounts of cloud resources. At each iteration, new assets are created and staged. At each release, workloads are readied for production promotion. Each of these cycles has the potential to introduce previously unidentified business risks.

Assuming a business risk MVP is the starting point for your initial cloud adoption efforts, governance can mature in parallel with your increasing use of cloud resources. When the cloud governance team operates in parallel with cloud adoption teams, the growth of business risks can be addressed as they're identified, providing a stable ongoing model for developing governance maturity.

Each asset staged can easily be classified according to risk. Data classification documents can be built or created in parallel with staging cycles. Risk profile and exposure points can likewise be documented. Over time an extremely clear view of business risk will come into focus across the organization.

With each iteration, the cloud governance team can work with the cloud strategy team to quickly communicate new risks, mitigation strategies, tradeoffs, and potential costs. This empowers business participants and IT leaders to partner in mature, well-informed decisions. Those decisions then inform policy maturity. When required, the policy changes produce new work items for the maturity of core infrastructure systems. When changes to staged systems are required, the cloud adoption teams have ample time to make changes, while the business tests the staged systems and develops a user adoption plan.

This approach minimizes risks, while empowering the team to move quickly. It also ensures that risks are promptly addressed and resolved before deployment.

## Next steps

Learn to evaluate risk tolerance during cloud adoption.

[Evaluate risk tolerance](#)

# Evaluate risk tolerance

11/9/2020 • 8 minutes to read • [Edit Online](#)

Every business decision creates new risks. Making an investment in anything creates risk of losses. New products or services create risks of market failure. Changes to current products or services could reduce market share. Cloud transformation does not provide a magical solution to everyday business risk. To the contrary, connected solutions (cloud or on-premises) introduce new risks. Deploying assets to any network connected facility also expands the potential threat profile by exposing security weaknesses to a much broader, global community. Fortunately, cloud providers are aware of the changes, increases, and addition of risks. They invest heavily to reduce and manage those risks on the behalf of their customers.

This article is not focused on cloud risks. Instead it discusses the business risks associated with various forms of cloud transformation. Later in the article, the discussion shifts focus to discuss ways of understanding the business's tolerance for risk.

## What business risks are associated with a cloud transformation?

True business risks are based on the details of specific transformations. Several common risks provide a conversation starter to understand business-specific risks.

### IMPORTANT

Before reading the following, be aware that each of these risks can be managed. The goal of this article is to inform and prepare readers for more productive risk management discussions.

- **Data breach:** The top risk associated with any transformation is a data breach. Data leaks can cause significant damage to your company, leading to loss of customers, decrease in business, or even legal liability. Any changes to the way data is stored, processed, or used creates risk. Cloud transformations create a high degree of change regarding data management, so the risk should not be taken lightly. The [Security Baseline discipline](#), [data classification](#), and [incremental rationalization](#) can each help manage this risk.
- **Service disruption:** Business operations and customer experiences rely heavily on technical operations. Cloud transformations will create change in IT operations. In some organizations, that change is small and easily adjusted. In other organizations, these changes could require retooling, retraining, or new approaches to support cloud operations. The bigger the change, the bigger the potential impact on business operations and customer experience. Managing this risk will require the involvement of the business in transformation planning. Release planning and first workload selection in the [incremental rationalization](#) article discuss ways to choose workloads for transformation projects. The business's role in that activity is to communicate the business operations risk of changing prioritized workloads. Helping IT choose workloads that have a lower impact on operations will reduce the overall risk.
- **Budget control:** Cost models change in the cloud. This change can create risks associated with cost overruns or increases in the cost of goods sold (COGS), especially directly attributed operating expenses. When business works closely with IT, it is feasible to create transparency regarding costs and services consumed by various business units, programs, or projects. The [Cost Management discipline](#) provides examples of ways business and IT can partner on this topic.

The above are a few of the most common risks mentioned by customers. The cloud governance team and the cloud adoption teams can begin to develop a risk profile, as workloads are migrated and readied for production

release. Be prepared for conversations to define, refine, and manage risks based on the desired business outcomes and transformation effort.

## Understand risk tolerance

Identifying risk is a fairly direct process. IT-related risks are generally standard across industries. Tolerance for these risks is specific to each organization. This is the point where business and IT conversations tend to get hung up. Each side of the conversation is essentially speaking a different language. The following comparisons and questions are designed to start conversations that help each party better understand and calculate risk tolerance.

## Simple use case for comparison

To help understand risk tolerance, let's examine customer data. If a company in any industry posts customer data on an unsecured server, the technical risk of that data being compromised or stolen is roughly the same.

Tolerance for that risk will vary wildly based on the nature and potential value of the data.

- Companies in healthcare and finance in the United States, are governed by rigid, third-party compliance requirements. It is assumed that personal data or healthcare-related data is extremely confidential. There are severe consequences for these types of companies, if they're involved in the risks scenario above. Their tolerance will be extremely low. Any customer data published inside or outside of the network must be governed by those third-party compliance policies.
- A gaming company whose customer data is limited to a user name, play times, and high scores is not as likely to suffer significant consequences beyond loss to reputation, if they engage in the risky behavior above. While any unsecured data is at risk, the impact of that risk is small. Therefore, the tolerance for risk in this case is high.
- A medium-sized enterprise that provides carpet-cleaning services to thousands of customers would fall in between these two tolerance extremes. Customer data may be more robust, containing details like addresses and phone numbers. Both are considered personal data and should be protected, but no specific governance requirement mandates that the data be secured. From an IT perspective, the answer is simple, secure the data. From a business perspective, it may not be as simple. The business would need more details before they could determine a level of tolerance for this risk.

The next section shares a few sample questions that could help the business determine a level of risk tolerance for the use case above or others.

## Risk tolerance questions

This section lists conversation provoking questions in three categories: loss impact, probability of loss, and remediation costs. When business and IT partner to address each of these areas, the decision to expend effort on managing risks and the overall tolerance to a particular risk can easily be determined.

**Loss impact:** Questions to determine the impact of a risk. These questions can be difficult to answer. Quantifying the impact is best, but sometimes the conversation alone is enough to understand tolerance. Ranges are also acceptable, especially if they include assumptions that determined those ranges.

- Could this risk violate third-party compliance requirements?
- Could this risk violate internal corporate policies?
- Could this risk cause the loss of life, limb or property?
- Could this risk cost customers or market share? If so, can this cost be quantified?
- Could this risk create negative customer experiences? Are those experiences likely to affect sales or revenue?
- Could this risk create new legal liability? If so, is there a precedence for damage awards in these types of cases?
- Could this risk stop business operations? If so, how long would operations be down?

- Could this risk slow business operations? If so, how slow and how long?
- At this stage in the transformation is this a one-off risk or will it repeat?
- Does the risk increase or decrease in frequency as the transformation progresses?
- Does the risk increase or decrease in probability over time?
- Is the risk time sensitive in nature? Will the risk pass or get worse, if not addressed?

These basic questions will lead to many more. After exploring a healthy dialogue, it is suggested that the relevant risks be recorded and when possible quantified.

**Risk remediation costs:** Questions to determine the cost of removing or otherwise minimizing the risk. These questions can be fairly direct, especially when represented in a range.

- Is there a clear solution and what does it cost?
- Are there options for preventing or minimizing this risk? What is the range of costs for those solutions?
- What is needed from the business to select the best, clear solution?
- What is needed from the business to validate costs?
- What other benefits can come from the solution that would remove this risk?

These questions over simplify the technical solutions needed to manage or remove risks, but they communicate those solutions in ways the business can quickly integrate into a decision process.

**Probability of loss:** Questions to determine how likely it is that the risk will become a reality. This is the most difficult area to quantify. Instead it is suggested that the cloud governance team create categories for communicating probability, based on the supporting data. The following questions can help create categories that are meaningful to the team.

- Has any research been done regarding the likelihood of this risk being realized?
- Can the vendor provide references or statistics on the likelihood of an impact?
- Are there other companies in the relevant sector or vertical that have been hit by this risk?
- Look further, are there other companies in general that have been hit by this risk?
- Is this risk unique to something this company has done poorly?

After answering these questions along with questions as determined by the cloud governance team, groupings of probability will likely emerge. The following are a few grouping samples to help get started:

- **No indication:** Not enough research has been completed to determine probability.
- **Low risk:** Current research indicates realizing the risk is unlikely.
- **Future risk:** The current probability is low. Continued adoption would require a fresh analysis.
- **Medium risk:** It's likely that the risk will affect the business.
- **High risk:** Over time, it is increasingly likely that the business will realize this risk.
- **Declining risk:** The risk is medium to high. Actions in IT or the business are reducing the likelihood of an impact.

#### Determining tolerance:

The three question sets above should fuel enough data to determine initial tolerances. When risk and probability are low, and risk remediation costs are high, the business is unlikely to invest in remediation. When risk and probability are high, the business is likely to consider an investment, as long as the costs don't exceed the potential risks.

## Next steps

This type of conversation can help the business and IT evaluate tolerance more effectively. These conversations can be used during the creation of MVP policies and during incremental policy reviews.

Define corporate policy

# Define corporate policy for cloud governance

11/9/2020 • 3 minutes to read • [Edit Online](#)

Once you've analyzed the known risks and related risk tolerances for your organization's cloud transformation journey, your next step is to establish policy that will explicitly address those risks and define the steps needed to remediate them where possible.

## How can corporate IT policy become cloud-ready?

In traditional governance and incremental governance, corporate policy creates the working definition of governance. Most IT governance actions seek to implement technology to monitor, enforce, operate, and automate those corporate policies. Cloud governance is built on similar concepts.

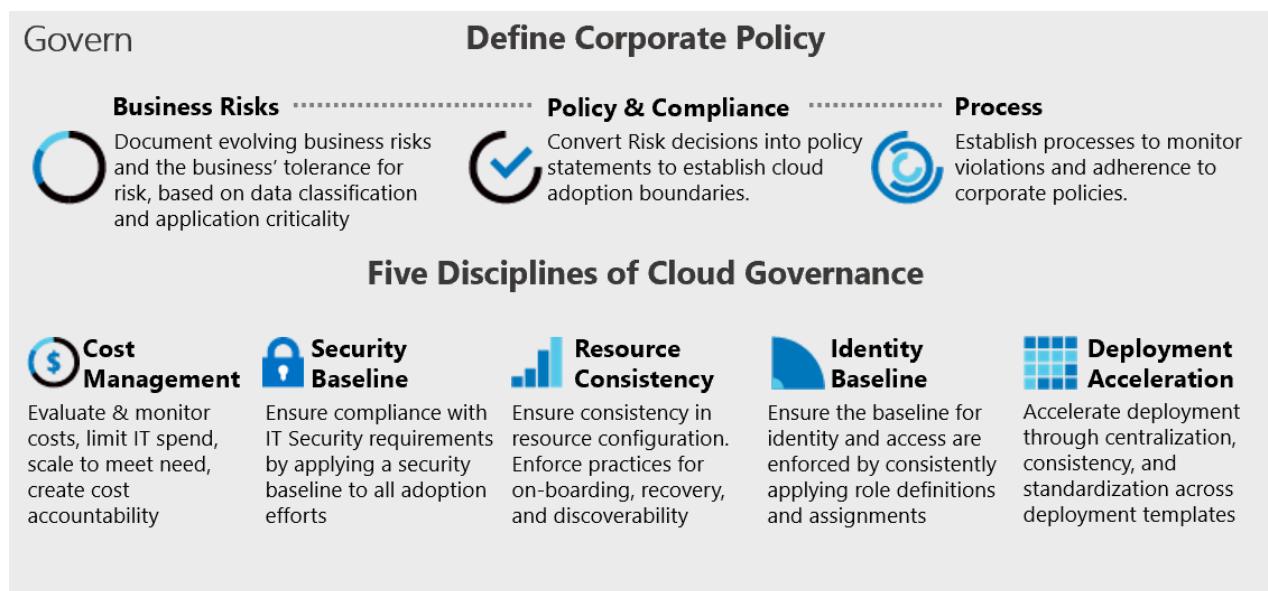


Figure 1: Corporate governance and governance disciplines.

The image above illustrates the relationship between business risk, policy and compliance, and monitoring and enforcement mechanisms that need to interact as part of your governance strategy. The Five Disciplines of Cloud Governance allow you to manage these interactions and realize your strategy.

Cloud governance is the product of an ongoing adoption effort over time, as a true lasting transformation doesn't happen overnight. Attempting to deliver complete cloud governance before addressing key corporate policy changes using a fast aggressive method seldom produces the desired results. Instead we recommend an incremental approach.

What is different about a Cloud Adoption Framework is the purchasing cycle and it can enable authentic transformation. Since there is not a large capital expenditure acquisition requirement, engineers can begin experimentation and adoption sooner. In most corporate cultures, elimination of the capital expense barrier to adoption can lead to tighter feedback loops, organic growth, and incremental execution.

The shift to cloud adoption requires a shift in governance. In many organizations, corporate policy transformation allows for improved governance and higher rates of adherence through incremental policy changes and automated enforcement of those changes, powered by newly defined capabilities that you configure with your cloud service provider.

## Review existing policies

As governance is an ongoing process, policy should be regularly reviewed with IT staff and stakeholders to ensure resources hosted in the cloud continue to maintain compliance with overall corporate goals and requirements. Your understanding of new risks and acceptable tolerance can fuel a [review of existing policies](#), in order to determine the required level of governance that is appropriate for your organization.

#### TIP

If your organization uses vendors or other trusted business partners, one of the biggest business risks to consider may be a lack of adherence to [regulatory compliance](#) by these external organizations. This risk often cannot be remediated, and instead may require a strict adherence to requirements by all parties. Make sure you've identified and understand any third-party compliance requirements before beginning a policy review.

## Create cloud policy statements

Cloud-based IT policies establish the requirements, standards, and goals that your IT staff and automated systems will need to support. Policy decisions are a primary factor in your [cloud architecture design](#) and how you will implement your [policy adherence processes](#).

Individual cloud policy statements are guidelines for addressing specific risks identified during your risk assessment process. While these policies can be integrated into your wider corporate policy documentation, cloud policy statements discussed throughout the Cloud Adoption Framework guidance tends to be a more concise summary of the risks and plans to deal with them. Each definition should include these pieces of information:

- **Business risk:** A summary of the risk this policy will address.
- **Policy statement:** A concise explanation of the policy requirements and goals.
- **Design or technical guidance:** Actionable recommendations, specifications, or other guidance to support and enforce this policy that IT teams and developers can use when designing and building their cloud deployments.

If you need help starting to define your policies, consult the [governance disciplines](#) introduced in the governance section overview. The articles for each of these disciplines includes examples of common business risks encountered when moving to the cloud and sample policies used to remediate those risks. For example, see the Cost Management discipline's [sample policy definitions](#).

## Incremental governance and integrating with existing policy

Planned additions to your cloud environment should always be vetted for compliance with existing policy, and policy updated to account for any issues not already covered. You should also perform regular [cloud policy review](#) to ensure your cloud policy is up-to-date and in-sync with any new corporate policy.

The need to integrate cloud policy with your legacy IT policies depends largely on the maturity of your cloud governance processes and the size of your cloud estate. See the article on [incremental governance and the policy MVP](#) for a broader discussion on dealing with policy integration during your cloud transformation.

## Next steps

After defining your policies, draft an architecture design guide to provide IT staff and developers with actionable guidance.

[Align your governance design guide with corporate policy](#)

# Align your cloud governance design guide with corporate policy

11/9/2020 • 2 minutes to read • [Edit Online](#)

After you've [defined cloud policies](#) based on your [identified risks](#), you'll need to generate actionable guidance that aligns with these policies for your IT staff and developers to refer to. Drafting a cloud governance design guide allows you to specify specific structural, technological, and process choices based on the policy statements you generated for each of the [five governance disciplines](#).

A cloud governance design guide should establish the architecture choices and design patterns for each of the core infrastructure components of cloud deployments that best meet your policy requirements. Alongside these you should provide a high-level explanation of the technology, tools, and processes that will support each of these design decisions.

Although your risk analysis and policy statements may, to some degree, be cloud platform agnostic, your design guide should provide platform-specific implementation details that your IT and dev teams can use when creating and deploying cloud-based workloads. Focus on the architecture, tools, and features of your chosen platform when making design decision and providing guidance.

While cloud design guides should take into account some of the technical details associated with each infrastructure component, they're not meant to be extensive technical documents or specifications. Make sure your guides address your policy statements and clearly state design decisions in a format easy for staff to understand and reference.

## Use the actionable governance guides

If you're planning to use the Azure platform for your cloud adoption, the Cloud Adoption Framework provides [actionable governance guides](#) illustrating the incremental approach of the Cloud Adoption Framework governance model. These narrative guides cover a range of common adoption scenarios, including the business risks, tolerance requirements, and policy statements that went into creating a governance minimum viable product (MVP). These guides represent a synthesis of real-world customer experience of the cloud adoption process in Azure.

While every cloud adoption has unique goals, priorities, and challenges, these samples should provide a good template for converting your policy into guidance. Pick the closest scenario to your situation as a starting point, and mold it to fit your specific policy needs.

## Next steps

With design guidance in place, establish policy adherence processes to ensure policy compliance.

[Establish policy adherence processes](#)

# Establish policy adherence processes

11/9/2020 • 5 minutes to read • [Edit Online](#)

After establishing your cloud policy statements and drafting a design guide, you'll need to create a strategy for ensuring your cloud deployment stays in compliance with your policy requirements. This strategy will need to encompass your cloud governance team's ongoing review and communication processes, establish criteria for when policy violations require action, and defining the requirements for automated monitoring and compliance systems that will detect violations and trigger remediation actions.

See the corporate policy sections of the [actionable governance guides](#) for examples of how policy adherence process fit into a cloud governance plan.

## Prioritize policy adherence processes

How much investment in developing processes is required to support your policy goals? Depending on the size and maturity of your cloud deployment, the effort required to establish processes that support compliance, and the costs associated with this effort, can vary widely.

For small deployments consisting of development and test resources, policy requirements may be simple and require few dedicated resources to address. On the other hand, a mature mission-critical cloud deployment with high-priority security and performance needs may require a team of staff, extensive internal processes, and custom monitoring tooling to support your policy goals.

As a first step in defining your policy adherence strategy, evaluate how the processes discussed below can support your policy requirements. Determine how much effort is worth investing in these processes, and then use this information to establish realistic budget and staffing plans to meet these needs.

## Establish cloud governance team processes

Before defining triggers for policy compliance remediation, you need establish the overall processes that your team will use and how information will be shared and escalated between IT staff and the cloud governance team.

### Assign cloud governance team members

Your cloud governance team will provide ongoing guidance on policy compliance and handle policy-related issues that emerge when deploying and operating your cloud assets. When building this team, invite staff members that have expertise in areas covered by your defined policy statements and identified risks.

For initial test deployments, this can be limited to a few system administrators responsible for establishing the basics of governance. As your governance processes mature, review the cloud guidance team's membership regularly to ensure that you can properly address new potential risks and policy requirements. Identify members of your IT and business staff with relevant experience or interest in specific areas of governance and include them in your teams on a permanent or temporary basis as needed.

### Reviews and policy iteration

As additional resources and workloads are deployed, the cloud governance team will need to ensure that new workloads or assets comply with policy requirements. Evaluate new requirements from workload development teams to ensure their planned deployments will align with your design guides, and update your policies to support these requirements when appropriate.

Plan to evaluate new potential risks and update policy statements and design guides as needed. Work with IT staff and workload teams to evaluate new Azure features and services on an ongoing basis. Also schedule regular

review cycles each of the five governance disciplines to ensure policy is current and in compliance.

## Education

Policy compliance requires IT staff and developers to understand the policy requirements that affect their areas of responsibility. Plan to devote resources to document decisions and requirements, and educate all relevant teams on the design guides that support your policy requirements.

As policy changes, regularly update documentation and training materials, and ensure education efforts communicate updated requirements and guidance to relevant IT staff.

At various stages of your cloud journey, you may find it best to consult with partners and professional training programs to enhance the education of your team, both technically, and procedurally. Additionally, many find that formal certifications are a valuable addition to your education portfolio and should be considered.

## Establish escalation paths

If a resource goes out of compliance, who gets notified? If IT staff detect a policy compliance issue, who do they contact? Make sure the escalation process to the cloud governance team is clearly defined. Ensure these communication channels are kept updated to reflect staff and organization changes.

# Violation triggers and actions

After defining your cloud governance team and its processes, you need to explicitly define what qualifies as compliance violations that will trigger actions, and what those actions should be.

## Define triggers

For each of your policy statements, review requirements to determine what constitutes a policy violation. Generate your triggers using the information you've already established as part of the policy definition process.

- **Risk tolerance:** Create violation triggers based on the metrics and risk indicators you established as part of your [risk tolerance analysis](#).
- **Defined policy requirements:** Policy statements may provide service-level agreement (SLA), business continuity and disaster recovery (BCDR), or performance requirements that should be used as the basis for compliance triggers.

## Define actions

Each violation trigger should have a corresponding action. Triggered actions should always notify an appropriate IT staff or cloud governance team member when a violation occurs. This notification can lead to a manual review of the compliance issue or kickoff a predefined remediation process depending on the type and severity of the detected violation.

Some examples of violation triggers and actions:

GOVERNANCE DISCIPLINE	SAMPLE TRIGGER	SAMPLE ACTION
Cost Management	Monthly cloud spending is more than 20% higher than expected.	Notify the billing unit leader who will begin a review of resource usage.
Security Baseline	Detect suspicious user activity.	Notify the IT security team and disable the suspect user account.
Resource Consistency	CPU utilization for a workload is greater than 90%.	Notify the IT operations team and scale out additional resources to handle the load.

# Automation of monitoring and compliance

After you've defined your compliance violation triggers and actions, you can start planning how best to use the logging and reporting tools and other features of the cloud platform to help automate your monitoring and policy compliance strategy.

For help choosing the best monitoring pattern for your deployment, see the [Logging and reporting decision guide](#).

## Next steps

Learn more about regulatory compliance in the cloud.

[Regulatory compliance](#)

# Introduction to regulatory compliance

11/9/2020 • 3 minutes to read • [Edit Online](#)

This is an introductory article about regulatory compliance, therefore it's not intended for implementing a compliance strategy. More detailed information about [Azure compliance offerings](#) is available at the [Microsoft Trust Center](#). Moreover, all downloadable documentation is available to certain Azure customers from the [Microsoft Service Trust Portal](#).

Regulatory compliance refers to the discipline and process of ensuring that a company follows the laws enforced by governing bodies in their geography or rules required by voluntarily adopted industry standards. For IT regulatory compliance, people and processes monitor corporate systems in an effort to detect and prevent violations of policies and procedures established by these governing laws, regulations, and standards. This in turn applies to a wide array of monitoring and enforcement processes. Depending on the industry and geography, these processes can become lengthy and complex.

Compliance is challenging for multinational organizations, especially in heavily regulated industries like healthcare and financial services. Standards and regulations abound, and in certain cases may change frequently, making it difficult for businesses to keep up with changing international electronic data handling laws.

As with security controls, organizations should understand the division of responsibilities regarding regulatory compliance in the cloud. Cloud providers strive to ensure that their platforms and services are compliant. Organizations also need to confirm that their applications, the infrastructure those applications depend on, and services supplied by third parties are also certified as compliant.

The following are descriptions of compliance regulations in various industries and geographies:

## HIPAA

A healthcare application that processes protected health information (PHI) is subject to both the privacy rule and the security rule encompassed within the Health Information Portability and Accountability Act (HIPAA). At a minimum, HIPAA could likely require that a healthcare business must receive written assurances from the cloud provider that it will safeguard any PHI received or created.

## PCI

The Payment Card Industry Data Security Standard (PCI DSS) is a proprietary information security standard for organizations that handle branded credit cards from the major card payment systems, including Visa, Mastercard, American Express, Discover, and JCB. The PCI standard is mandated by the card brands and administered by the Payment Card Industry Security Standards Council. The standard was created to increase controls around cardholder data to reduce credit-card fraud. Validation of compliance is performed annually, either by an external qualified security assessor (QSA) or by a firm-specific internal security assessor (ISA) who creates a report on compliance (ROC) for organizations handling large volumes of transactions, or by a self-assessment questionnaire (SAQ) for companies.

## Personal data

Personal data is information that could be used to identify a consumer, employee, partner, or any other living or legal entity. Many emerging laws, particularly those dealing with privacy and personal data, require that businesses themselves comply and report on compliance and any breaches that might occur.

## GDPR

One of the most important developments in this area is the General Data Protection Regulation (GDPR), designed to strengthen data protection for individuals within the European Union. GDPR requires that data about individuals (such as "a name, a home address, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer's IP address") be maintained on servers within the EU and not transferred out of it. It also requires that companies notify individuals of any data breaches, and mandates that companies have a data protection officer (DPO). Other countries have, or are developing, similar types of regulations.

## Compliant foundation in Azure

To help customers meet their own compliance obligations across regulated industries and markets worldwide, Azure maintains the largest compliance portfolio in the industry, in breadth (total number of offerings) as well as depth (number of customer-facing services in assessment scope). Azure compliance offerings are grouped into four segments:

- Global
- US government
- Industry
- Regional

Azure compliance offerings are based on various types of assurances, including formal certifications, attestations, validations, authorizations, and assessments produced by independent third-party auditing firms, as well as contractual amendments, self-assessments, and customer guidance documents produced by Microsoft. Each offering description in this document provides an up-to-date scope statement indicating which Azure customer-facing services are in scope for the assessment, as well as links to downloadable resources to assist customers with their own compliance obligations.

The Microsoft Trust Center provides more detailed information about [Azure compliance offerings](#). Additionally, all downloadable documentation is available to certain Azure customers from the [Microsoft Service Trust Portal](#) in the following sections:

- **Audit reports:** Includes sections for FedRAMP, GRC assessment, ISO, PCI DSS, and SOC reports.
- **Data protection resources:** Includes compliance guides, FAQ and white papers, and pen test and security assessment sections.

## Next steps

Learn more about cloud security readiness.

[Cloud security readiness](#)

# CISO cloud readiness guide

11/9/2020 • 3 minutes to read • [Edit Online](#)

Microsoft guidance like the Cloud Adoption Framework is not positioned to determine or guide the unique security constraints of the thousands of enterprises supported by this documentation. When moving to the cloud, the role of the chief information security officer or chief information security office (CISO) isn't supplanted by cloud technologies. Quite the contrary, the CISO and the office of the CISO, become more engrained and integrated. This guide assumes the reader is familiar with CISO processes and is seeking to modernize those processes to enable cloud transformation.

Cloud adoption enables services that weren't often considered in traditional IT environments. Self-service or automated deployments are commonly executed by application development or other IT teams not traditionally aligned to production deployment. In some organizations, business constituents similarly have self-service capabilities. This can trigger new security requirements that weren't needed in the on-premises world. Centralized security is more challenging, security often becomes a shared responsibility across the business and IT culture. This article can help a CISO prepare for that approach and engage in incremental governance.

## How can a CISO prepare for the cloud?

Like most policies, security and governance policies within an organization tend to grow organically. When security incidents happen, they shape policy to inform users and reduce the likelihood of repeat occurrences. While natural, this approach creates policy bloat and technical dependencies. Cloud transformation journeys create a unique opportunity to modernize and reset policies. While preparing for any transformation journey, the CISO can create immediate and measurable value by serving as the primary stakeholder in a [policy review](#).

In such a review, the role of the CISO is to create a safe balance between the constraints of existing policy/compliance and the improved security posture of cloud providers. Measuring this progress can take many forms, often it is measured in the number of security policies that can be safely offloaded to the cloud provider.

**Transferring security risks:** As services are moved into infrastructure as a service (IaaS) hosting models, the business assumes less direct risk regarding hardware provisioning. The risk isn't removed, instead it is transferred to the cloud vendor. Should a cloud vendor's approach to hardware provisioning provide the same level of risk mitigation, in a secure repeatable process, the risk of hardware provisioning execution is removed from corporate IT's area of responsibility and transferred to the cloud provider. This reduces the overall security risk corporate IT is responsible for managing, although the risk itself should still be tracked and reviewed periodically.

As solutions move further "up stack" to incorporate platform as a service (PaaS) or software as a service (SaaS) models, additional risks can be avoided or transferred. When risk is safely moved to a cloud provider, the cost of executing, monitoring, and enforcing security policies or other compliance policies can be safely reduced as well.

**Growth mindset:** Change can be scary to both the business and technical implementors. When the CISO leads a growth mindset shift in an organization, we've found that those natural fears are replaced with an increased interest in safety and policy compliance. Approaching a [policy review](#), a transformation journey, or simple implementation reviews with a growth mindset, allows the team to move quickly but not at the cost of a fair and manageable risk profile.

## Resources for the chief information security officer

Knowledge about the cloud is fundamental to approaching a [policy review](#) with a growth mindset. The following resources can help the CISO better understand the security posture of Microsoft's Azure platform.

## **Security platform resources:**

- [Security development lifecycle, internal audits](#)
- [Mandatory security training, background checks](#)
- [Penetration testing, intrusion detection, DDoS, audits, and logging](#)
- [State-of-the-art datacenter, physical security, secure network](#)
- [Microsoft Azure Security Response in the Cloud \(PDF\)](#)

## **Privacy and controls:**

- [Manage your data all the time](#)
- [Control on data location](#)
- [Provide data access on your terms](#)
- [Responding to law enforcement](#)
- [Stringent privacy standards](#)

## **Compliance:**

- [Microsoft Trust Center](#)
- [Common controls hub](#)
- [Cloud Services Due Diligence Checklist](#)
- [Regional and country compliance](#)

## **Transparency:**

- [How Microsoft secures customer data in Azure services](#)
- [How Microsoft manages data location in Azure services](#)
- [Who in Microsoft can access your data on what terms](#)
- [Review certification for Azure services, transparency hub](#)

## **Next steps**

The first step to taking action in any governance strategy is a [policy review](#). Policy and compliance could be a useful guide during your policy review.

[Prepare for a policy review](#)

# Conduct a cloud policy review

11/9/2020 • 3 minutes to read • [Edit Online](#)

A cloud policy review is the first step toward [governance maturity](#) in the cloud. The objective of this process is to modernize existing corporate IT policies. When completed, the updated policies provide an equivalent level of risk management for cloud-based resources. This article explains the cloud policy review process and its importance.

## Why perform a cloud policy review?

Most businesses manage IT through the execution of processes that align with governing policies. In small businesses, these policies may be anecdotal and processes loosely defined. As businesses grow into large enterprises, policies and processes tend to be more clearly documented and consistently executed.

As companies mature corporate IT policies, dependencies on past technical decisions have a tendency to seep into governing policies. For instance, it's common to see disaster recovery processes include policy that mandates offsite tape backups. This inclusion assumes a dependency on one type of technology (tape backups), that may no longer be the most relevant solution.

Cloud transformations create a natural inflection point to reconsider the legacy policy decisions of the past. Technical capabilities and default processes change considerably in the cloud, as do the inherent risks. Using the prior example, the tape backup policy stemmed from the risk of a single point of failure by keeping data in one location and the business need to minimize the risk profile by mitigating this risk. In a cloud deployment, there are several options that deliver the same risk mitigation, with much lower recovery time objectives (RTO). For example:

- A cloud-native solution could enable geo-replication of the Azure SQL Database.
- A hybrid solution could use Azure Site Recovery to replicate an IaaS workload to Azure.

When executing a cloud transformation, policies often govern many of the tools, services, and processes available to the cloud adoption teams. If those policies are based on legacy technologies, they may hinder the team's efforts to drive change. In the worst case, important policies are entirely ignored by the migration team to enable workarounds. Neither is an acceptable outcome.

## The cloud policy review process

Cloud policy reviews align existing IT governance and IT security policies with the [Five Disciplines of Cloud Governance](#):

- [Cost Management discipline](#)
- [Security Baseline discipline](#)
- [Identity Baseline discipline](#)
- [Resource Consistency discipline](#)
- [Deployment Acceleration discipline](#).

For each of these disciplines, the review process follows these steps:

1. Review existing on-premises policies related to the specific discipline, looking for two key data points: legacy dependencies and identified business risks.
2. Evaluate each business risk by asking a simple question: does the business risk still exist in a cloud model?
3. If the risk still exists, rewrite the policy by documenting the necessary business mitigation, not the technical

solution.

4. Review the updated policy with the cloud adoption teams to understand potential technical solutions to the required mitigation.

## Example of a policy review for a legacy policy

To provide an example of the process, let's again use the tape backup policy in the prior section:

- A corporate policy mandates offsite tape backups for all production systems. In this policy, you can see two data points of interest:
  - Legacy dependency on a tape backup solution.
  - An assumed business risk associated with the storage of backups in the same physical location as the production equipment.
- Does the risk still exist? Yes. Even in the cloud, a dependence on a single facility does create some risk. There is a lower probability of this risk affecting the business than was present in the on-premises solution, but the risk still exists.
- Rewrite of the policy. In the case of a datacenter-wide disaster, there must exist a means of restoring production systems within 24 hours of the outage in a different datacenter and different geographic location.
  - It is also important to consider that the timeline specified in the above requirement may have been set by technical constraints that are no longer present in the cloud. Make sure to understand the technical constraints and capabilities of the cloud before simply applying a legacy RTO/RPO.
- Review with the cloud adoption teams. Depending on the solution being implemented, there are multiple means of adhering to this Resource Consistency policy.

## Next steps

Learn more about including data classification in your cloud governance strategy.

[Data classification](#)

# What is data classification?

11/9/2020 • 2 minutes to read • [Edit Online](#)

Data classification allows you to determine and assign value to your organization's data and provides a common starting point for governance. The data classification process categorizes data by sensitivity and business impact in order to identify risks. When data is classified, you can manage it in ways that protect sensitive or important data from theft or loss.

## Understand data risks, then manage them

Before any risk can be managed, it must be understood. In the case of data breach liability, that understanding starts with data classification. Data classification is the process of associating a metadata characteristic to every asset in a digital estate, which identifies the type of data associated with that asset.

Any asset identified as a potential candidate for migration or deployment to the cloud should have documented metadata to record the data classification, business criticality, and billing responsibility. These three points of classification can go a long way to understanding and mitigating risks.

## Classifications Microsoft uses

The following is a list of classifications Microsoft uses. Depending on your industry or existing security requirements, data classification standards might already exist within your organization. If no standard exists, you might want to use this sample classification to better understand your own digital estate and risk profile.

- **Non-business:** Data from your personal life that doesn't belong to Microsoft.
- **Public:** Business data that is freely available and approved for public consumption.
- **General:** Business data that isn't meant for a public audience.
- **Confidential:** Business data that can cause harm to Microsoft if overshared.
- **Highly confidential:** Business data that would cause extensive harm to Microsoft if overshared.

## Tagging data classification in Azure

Resource tags are a good approach for metadata storage, and you can use these tags to apply data classification information to deployed resources. Although tagging cloud assets by classification isn't a replacement for a formal data classification process, it provides a valuable tool for managing resources and applying policy. [Azure Information Protection](#) is an excellent solution to help you classify data itself, regardless of where it resides (on-premises, in Azure, or somewhere else). Consider it as part of an overall classification strategy.

## Take action

Take action by defining and tagging assets with a defined data classification.

- [Choose one of the actionable governance guides](#) for examples of applying tags across your portfolio.
- Review the [naming and tagging standards](#) article to define a more comprehensive tagging standard.
- For additional information on resource tagging in Azure, see [Use tags to organize your Azure resources and management hierarchy](#).

## Next steps

Continue learning from this article series by reviewing the article on securing sensitive data. The next article

contains applicable insights if you are working with data that is classified as confidential or highly confidential.

[Secure sensitive data](#)

# The Five Disciplines of Cloud Governance

11/9/2020 • 2 minutes to read • [Edit Online](#)

Any change to business processes or technology platforms introduces risk. Cloud governance teams, whose members are sometimes known as cloud custodians, are tasked with mitigating these risks and ensuring minimal interruption to adoption or innovation efforts.

The Cloud Adoption Framework governance model guides these decisions, irrespective of the chosen cloud platform, by focusing on [development of corporate policy](#) and the [Five Disciplines of Cloud Governance](#).

[Actionable design guides](#) demonstrate this model using Azure services. Learn about the disciplines of the Cloud Adoption Framework governance model below.



Figure 1: Visual of corporate policy and the Five Disciplines of Cloud Governance.

## Disciplines of Cloud Governance

With any cloud platform, there are common governance disciplines that help inform policies and align toolchains. These disciplines guide decisions about the proper level of automation and enforcement of corporate policy across cloud platforms.

	<b>Cost Management:</b> Cost is a primary concern for cloud users. Develop policies for cost control for all cloud platforms.
	<b>Security Baseline:</b> Security is a complex subject, unique to each company. Once security requirements are established, cloud governance policies and enforcement apply those requirements across network, data, and asset configurations.
	<b>Identity Baseline:</b> Inconsistencies in the application of identity requirements can increase the risk of breach. The Identity Baseline discipline focuses ensuring that identity is consistently applied across cloud adoption efforts.
	<b>Resource Consistency:</b> Cloud operations depend on consistent resource configuration. Through governance tooling, resources can be configured consistently to manage risks related to onboarding, drift, discoverability, and recovery.



**Deployment Acceleration:** Centralization, standardization, and consistency in approaches to deployment and configuration improve governance practices. When provided through cloud-based governance tooling, they create a cloud factor that can accelerate deployment activities.

# Cost Management discipline overview

11/9/2020 • 2 minutes to read • [Edit Online](#)

The Cost Management discipline is one of the [Five Disciplines of Cloud Governance](#) within the [Cloud Adoption Framework governance model](#). For many customers, governing their costs is a major concern when adopting cloud technologies. Balancing performance demands, adoption pacing, and cloud services costs can be challenging. This is especially relevant during major business transformations that implement cloud technologies. This section outlines the approach to developing a Cost Management discipline as part of a cloud governance strategy.

## NOTE

Cost Management discipline does not replace the existing business teams, accounting practices, and procedures that are involved in your organization's financial management of IT-related costs. The primary purpose of this discipline is to identify potential cloud-related risks related to IT spending, and provide risk-mitigation guidance to the business and IT teams responsible for deploying and managing cloud resources.

The primary audience for this guidance is your organization's cloud architects and other members of your cloud governance team. The decisions, policies, and processes that emerge from this discipline should involve engagement and discussions with relevant members of your business and IT teams, especially those leaders responsible for owning, managing, and paying for cloud-based workloads.

## Policy statements

Actionable policy statements and the resulting architecture requirements serve as the foundation of a Cost Management discipline. Use [sample policy statements](#) as a starting point for defining your Cost Management policies.

### Caution

The sample policies come from common customer experiences. To better align these policies to specific cloud governance needs, execute the following steps to create policy statements that meet your unique business needs.

## Develop governance policy statements

The following steps help you define governance policies to control costs in your environment.



[Cost Management discipline template](#): Download the template for documenting a Cost Management discipline.



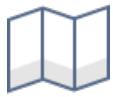
[Business risks](#): Understand the motives and risks commonly associated with the Cost Management discipline.



**Indicators and metrics:** Indicators to understand whether it is the right time to invest in the Cost Management discipline.



**Policy adherence processes:** Suggested processes for supporting policy compliance in the Cost Management discipline.



**Maturity:** Align cloud management maturity with phases of cloud adoption.



**Toolchain:** Azure services that can be implemented to support the Cost Management discipline.

## Next steps

Get started by evaluating business risks in a specific environment.

[Understand business risks](#)

# Cost Management discipline template

11/9/2020 • 2 minutes to read • [Edit Online](#)

The first step to implementing change is communicating the desired change. The same is true when changing governance practices. The template below serves as a starting point for documenting and communicating policy statements that govern cost management issues in the cloud.

As your discussions progress, use this template's structure as a model for capturing the business risks, risk tolerances, compliance processes, and tooling needed to define your organization's Cost Management policy statements.

## IMPORTANT

This template is a limited sample. Before updating this template to reflect your requirements, you should review the subsequent steps for defining an effective Cost Management discipline within your cloud governance strategy.

[Download the Cost Management discipline template](#)

## Next steps

Solid governance practices start with an understanding of business risk. Review the article on business risks and begin to document the business risks that align with your current cloud adoption plan.

[Understand business risks](#)

# Motivations and business risks in the Cost Management discipline

11/9/2020 • 2 minutes to read • [Edit Online](#)

This article discusses the reasons that customers typically adopt a Cost Management discipline within a cloud governance strategy. It also provides a few examples of business risks that drive policy statements.

## Relevance

In terms of cost governance, cloud adoption creates a paradigm shift. Managing costs in a traditional on-premises world is based on refresh cycles, datacenter acquisitions, host renewals, and recurring maintenance issues. You can forecast, plan, and refine these costs to align with annual capital expenditure budgets.

For cloud solutions, many businesses tend to take a more reactive approach to cost management. In many cases, businesses will prepurchase, or commit to use, a set amount of cloud services. This model assumes that maximizing discounts, based on how much the business plans on spending with a specific cloud vendor, creates the perception of a proactive, planned cost cycle. That perception will only become reality if the business also implements a mature Cost Management discipline.

The cloud offers self-service capabilities that were previously unheard of in traditional on-premises datacenters. These new capabilities empower businesses to be more agile, less restrictive, and more open to adopt new technologies. The downside of self-service is that end users can unknowingly exceed allocated budgets. Conversely, the same users can experience a change in plans and unexpectedly not use the amount of cloud services forecasted. The potential of shift in either direction justifies investment in a Cost Management discipline within the governance team.

## Business risk

The Cost Management discipline attempts to address core business risks related to expenses incurred when hosting cloud-based workloads. Work with your business to identify these risks and monitor each of them for relevance as you plan for and implement your cloud deployments.

Risks will differ between organization, but the following serve as common cost-related risks that you can use as a starting point for discussions within your cloud governance team:

- **Budget control:** Not controlling budget can lead to excessive spending with a cloud vendor.
- **Utilization loss:** Prepurchases or precommitments that go unused can result in lost investments.
- **Spending anomalies:** Unexpected spikes in either direction can be indicators of improper usage.
- **Overprovisioned assets:** When assets are deployed in a configuration that exceed the needs of an application or virtual machine (VM), they can create waste.

## Next steps

Use the [Cost Management policy template](#) to document business risks that are likely to be introduced by the current cloud adoption plan.

After you've gained an understanding of realistic business risks, the next step is to document the business's tolerance for risk and the indicators and key metrics to monitor that tolerance.

[Understand indicators, metrics, and risk tolerance](#)

# Risk tolerance metrics and indicators in the Cost Management discipline

11/9/2020 • 3 minutes to read • [Edit Online](#)

Learn to quantify business risk tolerance associated with the Cost Management discipline. Defining metrics and indicators helps to create a business case for investing in the maturity of this discipline.

## Metrics

Cost management generally focuses on metrics related to costs. As part of your risk analysis, you'll want to gather data related to your current and planned spending on cloud-based workloads to determine how much risk you face, and how important investment in your Cost Management discipline is for your planned cloud deployments.

The following are examples of useful metrics that you should gather to help evaluate risk tolerance within the Cost Management discipline:

- **Annual spending:** The total annual cost for services provided by a cloud provider.
- **Monthly spending:** The total monthly cost for services provided by a cloud provider.
- **Forecasted versus actual ratio:** The ratio comparing forecasted and actual spending (monthly or annual).
- **Pace of adoption (month-over-month) ratio:** The percentage of the delta in cloud costs from month to month.
- **Accumulated cost:** Total accrued daily spending, starting from the beginning of the month.
- **Spending trends:** Spending trend against the budget.

## Risk tolerance indicators

During early small-scale deployments, such as dev/test or experimental first workloads, cost management is likely to be of relatively low risk. As more assets are deployed, the risk grows and the business's tolerance for risk is likely to decline. Additionally, as more cloud adoption teams are given the ability to configure or deploy assets to the cloud, the risk grows and tolerance decreases. Conversely, developing a Cost Management discipline will take people from the cloud adoption phase to deploying more innovative technologies.

In the early stages of cloud adoption, you will work with your business to determine a risk tolerance baseline. Once you have a baseline, you will need to determine the criteria that would trigger an investment in the Cost Management discipline. These criteria will likely be different for every organization.

Once you have identified [business risks](#), you will work with your business to identify benchmarks that you can use to identify triggers that could potentially increase those risks. The following are a few examples of how metrics, such as those mentioned above, can be compared against your risk baseline tolerance to indicate your business's need to further invest in cost management.

- **Commitment-driven (most common):** A company that is committed to spending  $\$x,000,000$  this year on a cloud vendor. They need a Cost Management discipline to ensure that the business doesn't exceed its spending targets by more than 20%, and that they will use at least 90% of their commitment.
- **Percentage trigger:** A company with cloud spending that is stable for their production systems. If that changes by more than  $x\%$ , then a Cost Management discipline is a wise investment.
- **Overprovisioned trigger:** A company who believes their deployed solutions are overprovisioned. Cost management is a priority investment until they demonstrate proper alignment of provisioning and asset utilization.

- **Monthly spending trigger:** A company that spends over \$x,000 per month is considered a sizable cost. If spending exceeds that amount in a given month, they will need to invest in cost management.
- **Annual spending trigger:** A company with an IT R&D budget that allows for spending \$x,000 per year on cloud experimentation. They may run production workloads in the cloud, but they're still considered experimental solutions if the budget doesn't exceed that amount. If the budget is exceeded, they will need to treat the budget like a production investment and manage spending closely.
- **Operating expense-adverse (uncommon):** As a company, they're averse to operating expenses and will need cost management controls in place before deploying a dev/test workload.

## Next steps

Use the [Cost Management discipline template](#) to document metrics and tolerance indicators that align to the current cloud adoption plan.

Review sample Cost Management policies as a starting point to develop your own policies to address specific business risks aligned with your cloud adoption plans.

[Review sample policies](#)

# Cost Management sample policy statements

11/9/2020 • 3 minutes to read • [Edit Online](#)

Individual cloud policy statements are guidelines for addressing specific risks identified during your risk assessment process. These statements should provide a concise summary of risks and plans to deal with them. Each statement definition should include these pieces of information:

- **Business risk:** A summary of the risk this policy will address.
- **Policy statement:** A clear summary explanation of the policy requirements.
- **Design options:** Actionable recommendations, specifications, or other guidance that IT teams and developers can use when implementing the policy.

The following sample policy statements address common cost-related business risks. These statements are examples you can reference when drafting policy statements to address your organization's needs. These examples are not meant to be prescriptive, and there are potentially several policy options for dealing with each identified risk. Work closely with business and IT teams to identify the best policies for your unique set of risks.

## Future-proofing

**Business risk:** Current criteria that don't warrant an investment in a Cost Management discipline from the governance team, but you anticipate such an investment in the future.

**Policy statement:** You should associate all assets deployed to the cloud with a billing unit and application or workload. This policy will ensure that your Cost Management discipline is effective.

**Design options:** For information on establishing a future-proof foundation, see the discussions related to creating a governance MVP in the [actionable design guides](#) included as part of the Cloud Adoption Framework guidance.

## Budget overruns

**Business risk:** Self-service deployment creates a risk of overspending.

**Policy statement:** Any cloud deployment must be allocated to a billing unit with approved budget and a mechanism for budgetary limits.

**Design options:** In Azure, budget can be controlled with [Azure Cost Management + Billing](#).

## Underutilization

**Business risk:** The company has prepaid for cloud services or has made an annual commitment to spend a specific amount. There is a risk that the agreed-on amount won't be used, resulting in a lost investment.

**Policy statement:** Each billing unit with an allocated cloud budget will meet annually to set budgets, quarterly to adjust budgets, and monthly to allocate time for reviewing planned versus actual spending. Discuss any deviations greater than 20% with the billing unit leader monthly. For tracking purposes, assign all assets to a billing unit.

**Design options:**

- In Azure, planned versus actual spending can be managed via [Azure Cost Management + Billing](#).
- There are several options for grouping resources by billing unit. In Azure, a [resource consistency model](#) should be chosen in conjunction with the governance team and applied to all assets.

## Overprovisioned assets

**Business risk:** In traditional on-premises datacenters, it is common practice to deploy assets with extra capacity planning for growth in the distant future. The cloud can scale more quickly than traditional equipment. Assets in the cloud are also priced based on the technical capacity. There is a risk of the old on-premises practice artificially inflating cloud spending.

**Policy statement:** Any asset deployed to the cloud must be enrolled in a program that can monitor utilization and report any capacity in excess of 50% of utilization. Any asset deployed to the cloud must be grouped or tagged in a logical manner, so governance team members can engage the workload owner regarding any optimization of overprovisioned assets.

**Design options:**

- In Azure, [Azure Advisor](#) can provide optimization recommendations.
- There are several options for grouping resources by billing unit. In Azure, a [resource consistency model](#) should be chosen in conjunction with the governance team and applied to all assets.

## Overoptimization

**Business risk:** Effective cost management creates new risks. Optimization of spending is inverse to system performance. When reducing costs, there is a risk of overtightening spending and producing poor user experiences.

**Policy statement:** Any asset that directly affects customer experiences must be identified through grouping or tagging. Before optimizing any asset that affects customer experience, the cloud governance team must adjust optimization based on at least 90 days of utilization trends. Document any seasonal or event-driven bursts considered when optimizing assets.

**Design options:**

- In Azure, [Azure Monitor's insights features](#) can help with analysis of system utilization.
- There are several options for grouping and tagging resources based on roles. In Azure, you should choose a [resource consistency model](#) in conjunction with the governance team and apply this to all assets.

## Next steps

Use the samples mentioned in this article as a starting point to develop policies that address specific business risks that align with your cloud adoption plans.

To begin developing your own custom Cost Management policy statements, download the [Cost Management policy template](#).

To accelerate adoption of this discipline, choose the [actionable governance guide](#) that most closely aligns with your environment. Then modify the design to incorporate your specific corporate policy decisions.

Building on risks and tolerance, establish a process for governing and communicating Cost Management policy adherence.

[Establish policy compliance processes](#)

# Cost Management policy compliance processes

11/9/2020 • 3 minutes to read • [Edit Online](#)

This article discusses an approach to creating processes that support an effective [Cost Management discipline](#). Effective governance of cloud costs starts with recurring manual processes designed to support policy compliance. This requires regular involvement of the cloud governance team and interested business stakeholders to review and update policy and ensure policy compliance. In addition, many ongoing monitoring and enforcement processes can be automated or supplemented with tooling to reduce the overhead of governance and allow for faster response to policy deviation.

## Planning, review, and reporting processes

The best Cost Management tools in the cloud are only as good as the processes and policies that they support. The following is a set of example processes commonly involved in the Cost Management discipline. Use these examples as a starting point when planning the processes that will allow you to continue to update cost policy based on business change and feedback from the business teams, subject to cost governance guidance.

**Initial risk assessment and planning:** As part of your initial adoption of the Cost Management discipline, identify your core business risks and tolerances related to cloud costs. Use this information to discuss budget and cost-related risks with members of your business teams and develop a baseline set of policies for mitigating these risks to establish your initial governance strategy.

**Deployment planning:** Before deploying any asset, establish a forecasted budget based on expected cloud allocation. Ensure that ownership and accounting information for the deployment is documented.

**Annual planning:** On an annual basis, perform a roll-up analysis on all deployed and to-be-deployed assets. Align budgets by business units, departments, teams, and other appropriate divisions to empower self-service adoption. Ensure that the leader of each billing unit is aware of the budget and how to track spending.

This is the time to make a precommitment or prepurchase to maximize discounting. It is wise to align annual budgeting with the cloud vendor's fiscal year to further capitalize on year-end discount options.

**Quarterly planning:** On a quarterly basis, review budgets with each billing unit leader to align forecast and actual spending. If there are changes to the plan or unexpected spending patterns, align and reallocate the budget.

This quarterly planning process is also a good time to evaluate the current membership of your cloud governance team for knowledge gaps related to current or future business plans. Invite relevant staff and workload owners to participate in reviews and planning as either temporary advisors or permanent members of your team.

**Education and training:** On a bimonthly basis, offer training sessions to make sure business and IT staff are up-to-date on the latest Cost Management policy requirements. As part of this process review and update any documentation, guidance, or other training assets to ensure they're in sync with the latest corporate policy statements.

**Monthly reporting:** On a monthly basis, report actual spending against forecast. Notify billing leaders of any unexpected deviations.

These basic processes will help align spending and establish a foundation for the Cost Management discipline.

## Processes for ongoing monitoring

A successful Cost Management strategy depends on visibility into the past, current, and planned future cloud-related spending. Without the ability to analyze the relevant metrics and data of your existing costs, you cannot

identify changes in your risks or detect violations of your risk tolerances. The ongoing governance processes discussed above require quality data to ensure policy can be modified to better protect your infrastructure against changing business requirements and cloud usage.

Ensure that your IT teams have implemented automated systems for monitoring your cloud spending and usage for unplanned deviations from expected costs. Establish reporting and alerting systems to ensure prompt detection and mitigation of potential policy violations.

## Compliance violation triggers and enforcement actions

When violations are detected, you should take enforcement actions to realign with policy. You can automate most violation triggers using the tools outlined in the [Cost Management toolchain for Azure](#).

The following are examples of triggers:

- **Monthly budget deviations:** Discuss any deviations in monthly spending that exceed 20% forecast-versus-actual ratio with the billing unit leader. Record resolutions and changes in forecast.
- **Pace of adoption:** Any deviation at a subscription level exceeding 20% will trigger a review with billing unit leader. Record resolutions and changes in forecast.

## Next steps

Use the [Cost Management discipline template](#) to document the processes and triggers that align to the current cloud adoption plan.

For guidance on executing Cost Management policies in alignment with adoption plans, see [Cost Management discipline improvement](#).

[Cost Management discipline improvement](#)

# Cost Management discipline improvement

11/9/2020 • 4 minutes to read • [Edit Online](#)

The Cost Management discipline attempts to address core business risks related to expenses incurred when hosting cloud-based workloads. Within the Five Disciplines of Cloud Governance, the Cost Management discipline is involved in controlling cost and usage of cloud resources with the goal of creating and maintaining a planned cost cycle.

This article outlines potential tasks your company perform to develop and mature your Cost Management discipline. These tasks can be broken down into planning, building, adopting, and operating phases of implementing a cloud solution. The tasks are then iterated on to allow the development of an [incremental approach to cloud governance](#).

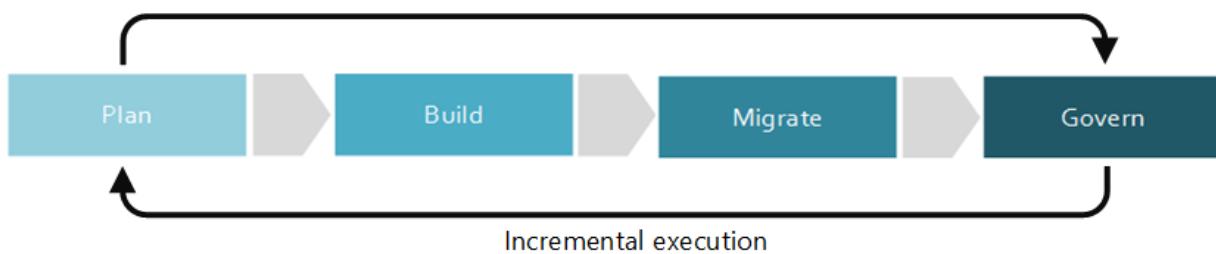


Figure 1: Phases of an incremental approach to cloud governance.

No single document can account for the requirements of all businesses. As such, this article outlines suggested minimum and potential example activities for each phase of the governance maturation process. The initial objective of these activities is to help you build a [policy MVP](#) and establish a framework for incremental policy improvement. Your cloud governance team will need to decide how much to invest in these activities to improve your Cost Management discipline capabilities.

**Caution**

Neither the minimum or potential activities outlined in this article are aligned to specific corporate policies or third-party compliance requirements. This guidance is designed to help facilitate the conversations that will lead to alignment of both requirements with a cloud governance model.

## Planning and readiness

This phase of governance maturity bridges the divide between business outcomes and actionable strategies. During this process, the leadership team defines specific metrics, maps those metrics to the digital estate, and begins planning the overall migration effort.

### Minimum suggested activities:

- Evaluate your [Cost Management toolchain](#) options.
- Develop a draft document for architecture guidelines and distribute to key stakeholders.
- Educate and involve the people and teams affected by the development of architecture guidelines.

### Potential activities:

- Ensure budgetary decisions that support the business justification for your cloud strategy.
- Validate learning metrics that you use to report on the successful allocation of funding.
- Understand the desired cloud accounting model that affects how cloud costs should be accounted for.
- Become familiar with the digital estate plan and validate accurate costing expectations.

- Evaluate buying options to determine whether it's better to "pay as you go" or to make a precommitment by purchasing an Enterprise Agreement.
- Align business goals with planned budgets and adjust budgetary plans as necessary.
- Develop a goals and budget reporting mechanism to notify technical and business stakeholders at the end of each cost cycle.

## Build and predeployment

Several technical and nontechnical prerequisites are required to successfully migrate an environment. This process focuses on the decisions, readiness, and core infrastructure that proceeds a migration.

### Minimum suggested activities:

- Implement your [Cost Management toolchain](#) by rolling out in a predeployment phase.
- Update the architecture guidelines document and distribute to key stakeholders.
- Develop educational materials and documentation, awareness communications, incentives, and other programs to help drive user adoption.
- Determine whether your purchase requirements align with your budgets and goals.

### Potential activities:

- Align your budgetary plans with the [subscription strategy](#) that defines your core ownership model.
- Use the [Resource Consistency discipline strategy](#) to enforce architecture and cost guidelines over time.
- Determine whether any cost anomalies affect your adoption and migration plans.

## Adopt and migrate

Migration is an incremental process that focuses on the movement, testing, and adoption of applications or workloads in an existing digital estate.

### Minimum suggested activities:

- Migrate your [Cost Management toolchain](#) from predeployment to production.
- Update the architecture guidelines document and distribute to key stakeholders.
- Develop educational materials and documentation, awareness communications, incentives, and other programs to help drive user adoption.

### Potential activities:

- Implement your cloud accounting model.
- Ensure that your budgets reflect your actual spending during each release and adjust as necessary.
- Monitor changes in budgetary plans and validate with stakeholders if additional sign-offs are needed.
- Update changes to the architecture guidelines document to reflect actual costs.

## Operate and post-implementation

After the transformation is complete, governance and operations must live on for the natural lifecycle of an application or workload. This phase of governance maturity focuses on the activities that commonly come after the solution is implemented and the transformation cycle begins to stabilize.

### Minimum suggested activities:

- Customize your [Cost Management toolchain](#) based on your organization's changing needs.
- Consider automating any notifications and reports to reflect actual spending.
- Refine architecture guidelines to guide future adoption processes.

- Educate affected teams on a periodic basis to ensure ongoing adherence to the architecture guidelines.

#### Potential activities:

- Execute a quarterly cloud business review to communicate value delivered to the business and associated costs.
- Adjust plans quarterly to reflect changes to actual spending.
- Determine financial alignment to P&Ls for business unit subscriptions.
- Analyze stakeholder value and cost reporting methods on a monthly basis.
- Remediate underused assets and determine whether they're worth continuing.
- Detect misalignments and anomalies between the plan and actual spending.
- Assist the cloud adoption teams and the cloud strategy team with understanding and resolving these anomalies.

## Next steps

Now that you understand the concept of cloud cost governance, review the Cost Management discipline best practices to find ways to reduce your overall spend.

[Cost Management discipline best practices](#)

# Best practices for costing and sizing resources hosted in Azure

11/9/2020 • 22 minutes to read • [Edit Online](#)

While delivering the disciplines of governance, cost management is a recurring theme at the enterprise level. By optimizing and managing costs, you can ensure the long-term success of your Azure environment. It's critical that all teams (such as finance, management, and application development teams) understand associated costs and review them on a recurring basis.

## IMPORTANT

The best practices and opinions described in this article are based on platform and service features in Azure that were available at the time of writing. Features and capabilities change over time. Not all recommendations will apply to your deployment, so choose what works best for your situation.

## Best practices by team and accountability

Cost management across the enterprise is a cloud governance and cloud operation function. All cost management decisions result in a change to the assets which support a workload. When those changes impact the architecture of a workload, additional considerations are required to minimize the impact on end users and business functions. The cloud adoption team who configured or developed that workload are likely to hold accountability for completing those types of changes.

- **Tagging is critical to all governance.** Ensure all workloads and resources follow [proper naming and tagging conventions](#) and [enforce tagging conventions using Azure Policy](#).
- **Identify right size opportunities.** Review your current resource utilization and performance requirements across the environment.
- **Resize:** Modify each resource to use the smallest instance or SKU that can support the performance requirements of each resource.
- **Horizontal over vertical scale.** Using multiple small instances can allow for an easier scaling path than a single larger instance. This allows for scale automation, which creates cost optimization.

## Operational cost management best practices

The following best practices are typically completed by a member of the cloud governance or cloud operations team, in accordance with patching and other scheduled maintenance processes. These best practices map to actionable guidance later in this article.

- **Tagging is critical to all governance:** Ensure all workloads and resources follow [proper naming and tagging conventions](#) and [enforce tagging conventions using Azure Policy](#).
- **Identify right size opportunities:** Review your current resource utilization and performance requirements across the environment to identify resources which have remained underutilized for a period of time (generally more than 90 days).
- **Right-size provisioned SKUs:** Modify underutilized resource to use the smallest instance or SKU that can support the performance requirements of each resource.
- **Auto-shutdown for VMs:** When a VM isn't in constant use, consider automated shutdown. The VM won't be deleted or decommissioned, but it will stop consuming compute and memory costs until it's turned back on.
- **Auto-shutdown all nonproduction assets:** If a VM is part of a nonproduction environment, specifically

development environments, establish an auto-shutdown policy to reduce unused costs. Whenever possible, use Azure DevTest Labs as a self-service option to help developers hold themselves accountable for cost.

- **Shut down and decommission unused resources:** Yes, we said it twice. If a resource hasn't been used in more than 90 days and doesn't have a clear uptime requirement, turn it off. More importantly, if a machine has been stopped or shut down for more than 90 days, then deprovision and delete that resource. Validate that any data retention policies are met through backup or other mechanisms.
- **Clean up orphaned disks:** Delete unused storage, especially VM storage that is no longer attached to any VMs.
- **Right-size redundancy:** If the resource doesn't require a high degree of redundancy, remove geo-redundant storage.
- **Adjust autoscale parameters:** Operational monitoring is likely to uncover usage patterns for various assets. When those usage patterns map to the parameters used to drive autoscale behaviors, it's common for the operations team to adjust autoscale parameters to meet seasonal demand or changes to budget allocations. Review workload cost management best practices for important precautions.

## Workload cost management best practices

Before making architectural changes, consult the technical lead for the workload. Facilitating a review of the workload using [Microsoft Azure Well-Architected Review](#) and the [Microsoft Azure Well-Architected Framework](#) to guide decisions regarding the following types of architectural changes.

- **Azure App Service.** Verify production requirements for any Premium tier App Service plans. Without an understanding of the business requirements for a workload and the underlying assets configuration, its difficult to determine whether a Premium tier plan is required.
- **Horizontal over vertical scale.** Using multiple small instances can allow for an easier scaling path than a single larger instance. This allows for scale automation, which creates cost optimization. Before a workload can scale horizontally, the technical team must verify that the application is idempotent. Achieving horizontal scale may first require changes to the code and configuration of various layers of the application.
- **Autoscale.** Enable autoscale on all app services to allow for a burstable number of smaller VMs. Enabling autoscale has the same idempotent requirement, which requires an understanding of the workload architecture. The workload and supporting assets must be approved for horizontal scaling and autoscaling by the adoption team, prior to any operational changes.
- **Implement serverless technologies:** VM workloads are often migrated "as is" to avoid downtime. Often VMs may host tasks that are intermittent, taking a short period to run, or alternatively many hours. For example, VMs that run scheduled tasks such as Windows task scheduler or PowerShell scripts. When these tasks aren't running, you're nevertheless absorbing VM and disk storage costs. After migration, consider rearchitecting layers of the workload to serverless technologies such as Azure Functions or Azure Batch jobs.

## Actionable best practices

The remainder of this article provides tactical examples of operational best practices that a cloud governance or cloud operations team can follow to optimize cost across the enterprise.

### Before adoption

Before you move your workloads to the cloud, estimate the monthly cost of running them in Azure. Proactively managing cloud costs helps you adhere to your operating expense budget. The best practices in this section help you to estimate costs, and perform right-sizing for VMs and storage before a workload is deployed to the cloud.

### Best practice: Estimate monthly workload costs

To forecast your monthly bill for Azure resources, there are several tools you can use.

- **Azure pricing calculator:** Select the products you want to estimate, for example VMs and storage, then input costs into the calculator to build an estimate.

**Billing Option**

Save up to 72% on pay-as-you-go prices with 1-year or 3-year Reserved Virtual Machine Instances. Reserved Instances are great for applications with steady-state usage and applications that require reserved capacity. [Learn more about Reserved VM Instances pricing.](#)

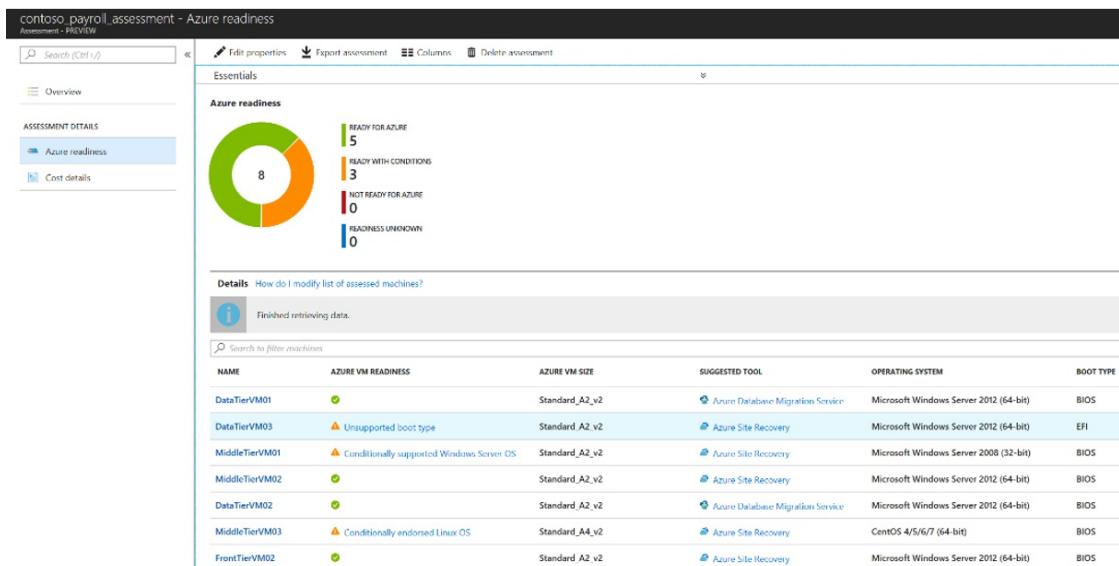
Pay as you go  
 1 year reserved (~38% savings)  
 3 year reserved (~59% savings)

**12**  
 Virtual machines

**\$1,350.97**  
Effective cost per month

*Azure pricing calculator.*

- **Azure Migrate:** To estimate costs, you need to review and account for all the resources required to run your workloads in Azure. To acquire this data, you create inventory of your assets, including servers, VMs, databases, and storage. You can use Azure Migrate to collect this information.
  - Azure Migrate discovers and assesses your on-premises environment to provide an inventory.
  - Azure Migrate can map and show you dependencies between VMs so that you have a complete picture.
  - An Azure Migrate assessment contains estimated cost.
    - **Compute costs:** Using the Azure VM size recommended when you create an assessment, Azure Migrate uses the Azure Billing APIs to calculate estimated monthly VM costs. The estimate considers the operating system, Software Assurance, Azure Reserved VM Instances, VM uptime, location, and currency settings. It aggregates the cost across all VMs in the assessment, and calculates a total monthly compute cost.
    - **Storage cost:** Azure Migrate calculates total monthly storage costs by aggregating the storage costs of all VMs in an assessment. You can calculate the monthly storage cost for a specific machine by aggregating the monthly cost of all disks attached to it.



### Azure Migrate assessment.

#### Learn more:

- Use the [Azure pricing calculator](#).
- Read the [Azure Migrate overview](#).
- Read about [Azure Migrate assessments](#).
- Learn more about the [Azure Database Migration Service](#).

## Best practice: Right-size VMs

You can choose various options when you deploy Azure VMs to support workloads. Each VM type has specific features and different combinations of CPU, memory, and disks. VMs are grouped as shown below:

Type	Details	Usage
General-purpose	Balanced CPU-to-memory.	Good for testing and development, small to midsize databases, low- to medium-volume traffic web servers.
Compute-optimized	High CPU-to-memory.	Good for medium-volume traffic web server, network appliances, batch processes, application servers.
Memory-optimized	High memory-to-CPU.	Good for relational databases, medium- to large-size cache, in-memory analytics.
Storage optimized	High disk throughput and I/O.	Suitable for big data, SQL, and NoSQL databases.
GPU optimized	Specialized VMs. Single or multiple GPUs.	Heavy graphics and video editing.
High performance	Fastest and most powerful CPU. VMs with optional high-throughput network interfaces (RDMA).	Critical high-performance applications.

- It's important to understand the pricing differences between these VMs, and the long-term budget effects.
- Each type has several VM series within it.

- Additionally, when you select a VM within a series, you can only scale the VM up and down within that series. For example, a `DS2_v2` instance can scale up to `DS4_v2`, but it can't be changed to an instance of a different series such as a `F2S_v2` instance.

#### Learn more:

- Learn more about [VM types and sizing](#), and map sizes to types.
- Plan [VM sizing](#).
- Review a [sample assessment for the fictional Contoso company](#).

## Best practice: Select the right storage

Tuning and maintaining on-premises storage (SAN or NAS), and the networks to support them, can be costly and time-consuming. File (storage) data is commonly migrated to the cloud to help alleviate operational and management headaches. Microsoft provides several options for moving data to Azure, and you need to make decisions about those options. Picking the right storage type for data can save your organization several thousands of dollars every month. A few considerations:

- Data that isn't accessed much and isn't business-critical shouldn't be placed on the most expensive storage.
- Conversely, important business-critical data should be located on higher tier storage options.
- During adoption planning, take an inventory of data and classify it by importance, in order to map it to the most suitable storage. Consider budget and costs, as well as performance. Cost shouldn't necessarily be the main decision-making factor. Picking the least expensive option could expose the workload to performance and availability risks.

### Storage data types

Azure provides different types of storage data.

DATA TYPE	DETAILS	USAGE
Blobs	Optimized to store massive amounts of unstructured objects, such as text or binary data.	Access data from everywhere over HTTP/HTTPS.  Use for streaming and random access scenarios. For example, to serve images and documents directly to a browser, stream video and audio, and store backup and disaster recovery data.
Files	Managed file shares accessed over SMB 3.0.	Use when migrating on-premises file shares, and to provide multiple access and connections to file data.
Disks	Based on page blobs.  Disk type (speed): Standard HDD, standard SSD, premium SSD, or ultra disks.  Disk management: unmanaged (you manage disk settings and storage) or managed (you select the disk type and Azure manages the disk for you).	Use premium disks for VMs. Use managed disks for simple management and scaling.
Queues	Store and retrieve large numbers of messages accessed via authenticated calls (HTTP or HTTPS).	Connect application components with asynchronous message queueing.

DATA TYPE	DETAILS	USAGE
Tables	Store tables.	Now part of Azure Cosmos DB Table API.

## Access tiers

Azure Storage provides different options for accessing block blob data. Selecting the right access tier helps ensure that you store block blob data in the most cost-effective manner.

ACCESS TIER	DETAILS	USAGE
Hot	<p>Higher storage costs, lower access, and transaction costs</p> <p>This is the default access tier.</p>	Use for data in active use that's accessed frequently.
Cool	<p>Lower storage costs, higher access and transaction costs.</p> <p>Store for minimum of 30 days.</p>	Store short-term, data is available but accessed infrequently.
Archive	<p>Used for individual block blobs.</p> <p>Most cost-effective option for storage. Lowest storage costs, highest access and transaction costs.</p>	Use for data that can tolerate several hours of retrieval latency and will reside in the archive tier for at least 180 days.

## Storage account types

Azure provides different types of storage accounts and performance tiers.

ACCOUNT TYPE	DETAILS	USAGE
General-purpose v2 Standard tier	<p>Supports blobs (block, page, append), files, disks, queues, and tables.</p> <p>Supports hot, cool, and archive access tiers. Zone-redundant storage (ZRS) is supported.</p>	Use for most scenarios and most types of data. Standard storage accounts can be HDD or SSD-based.
General-purpose v2 Premium tier	<p>Supports Blob storage data (page blobs). Supports hot, cool, and archive access tiers. ZRS is supported.</p> <p>Stored on SSD.</p>	Microsoft recommends using for all VMs.
General-purpose v1	Access tiering isn't supported. Doesn't support ZRS	Use if applications need the Azure classic deployment model.
Blob	<p>Specialized storage account for storing unstructured objects. Provides block blobs and append blobs only (no file, queue, table, or disk storage services).</p> <p>Provides the same durability, availability, scalability, and performance as general-purpose v2.</p>	You can't store page blobs in these accounts, and therefore can't store VHD files. You can set an access tier to hot or cool.

## Storage redundancy options

Storage accounts can use different types of redundancy for resilience and high availability.

Type	Details	Usage
Locally redundant storage (LRS)	Protects against a local outage by replicating within a single storage unit to a separate fault domain and update domain. Keeps multiple copies of your data in one datacenter. Provides at least 99.99999999 percent (eleven 9's) durability of objects over a given year.	Consider whether your application stores data that can be easily reconstructed.
Zone-redundant storage (ZRS)	Protects against a datacenter outage by replicating across three storage clusters in a single region. Each storage cluster is physically separated and located in its own Availability Zone. Provides at least 99.9999999999 percent (twelve 9's) durability of objects over a given year by keeping multiple copies of your data across multiple datacenters or regions.	Consider whether you need consistency, durability, and high availability. Might not protect against a regional disaster when multiple zones are permanently affected.
Geo-redundant storage (GRS)	Protects against an entire region outage by replicating data to a secondary region that's hundreds of miles away from the primary. Provides at least 99.999999999999 percent (sixteen 9's) durability of objects over a given year.	Replica data isn't available unless Microsoft initiates a failover to the secondary region. If failover occurs, read and write access is available.
Read-access geo-redundant storage (RA-GRS)	Similar to GRS. Provides at least 99.999999999999 percent (sixteen 9's) durability of objects over a given year.	Provides and 99.99 percent read availability by allowing read access from the second region used for GRS.

#### Learn more:

- Review [Azure Storage pricing](#).
- Learn to use the [Azure Import/Export service](#) to securely import large amounts of data to Azure Blob storage and Azure Files.
- Compare [blobs, files, and disk storage data types](#).
- Learn more about [access tiers](#).
- Review [different types of storage accounts](#).
- Learn about [Azure Storage redundancy](#), including LRS, ZRS, GRS, and read-access GRS.
- Learn more about [Azure Files](#).

## After adoption

Prior to adoption, cost forecasts are dependent upon decisions made by workload owners and the cloud adoption team. While the governance team can aid in influencing those decisions, there's likely to be little action for the governance team to take.

Once resources are in production, data can be aggregated and trends analyzed at an environment level. This data will help the governance team make sizing and usage decisions independently, based on actual usage patterns and current state architecture.

- Analyze data to generate a budget baseline for Azure resource groups and resources.
- Identify patterns of use that would allow you to reduce size and stop or pause resources to further reduce your

costs.

Best practices in this section include using Azure Hybrid Benefit and Azure Reserved Virtual Machine Instances, reduce cloud spending across subscriptions, using Azure Cost Management + Billing for cost budgeting and analysis, monitoring resources and implementing resource group budgets, and optimizing monitoring, storage, and VMs.

## Best practice: Take advantage of Azure Hybrid Benefit

Due to years of software investment in systems such as Windows Server and SQL Server, Microsoft is in a unique position to offer customers value in the cloud, with substantial discounts that other cloud providers can't necessarily provide.

An integrated Microsoft on-premises/Azure product portfolio generates competitive and cost advantages. If you currently have an operating system or other software licensing through Software Assurance (SA), you can take those licenses with you to the cloud for with Azure Hybrid Benefit.

**Learn more:**

- [Take a look at the Azure Hybrid Benefit savings calculator.](#)
- Learn more about [Azure Hybrid Benefit for Windows Server](#).
- Review [pricing guidance for SQL Server Azure VMs](#).

## Best practice: Use Azure Reserved VM Instances

Most cloud platforms are set up as pay-as-you-go. This model presents disadvantages, since you don't necessarily know how dynamic workloads will be. When you specify clear intentions for a workload, you contribute to infrastructure planning.

Using Azure Reserved VM Instances, you prepay for either a one-year or three-year term for reserved instances.

- Prepayment provides a discount on the resources you use.
- You can significantly reduce costs for VM compute, SQL Database compute, Azure Cosmos DB, or other resources by up to 72% on pay-as-you-go prices.
- Reserved instances provide a billing discount, and don't affect the runtime state of your resources.
- You can cancel reserved instances.

# Save up to **80%** with RIs and Azure Hybrid Benefit

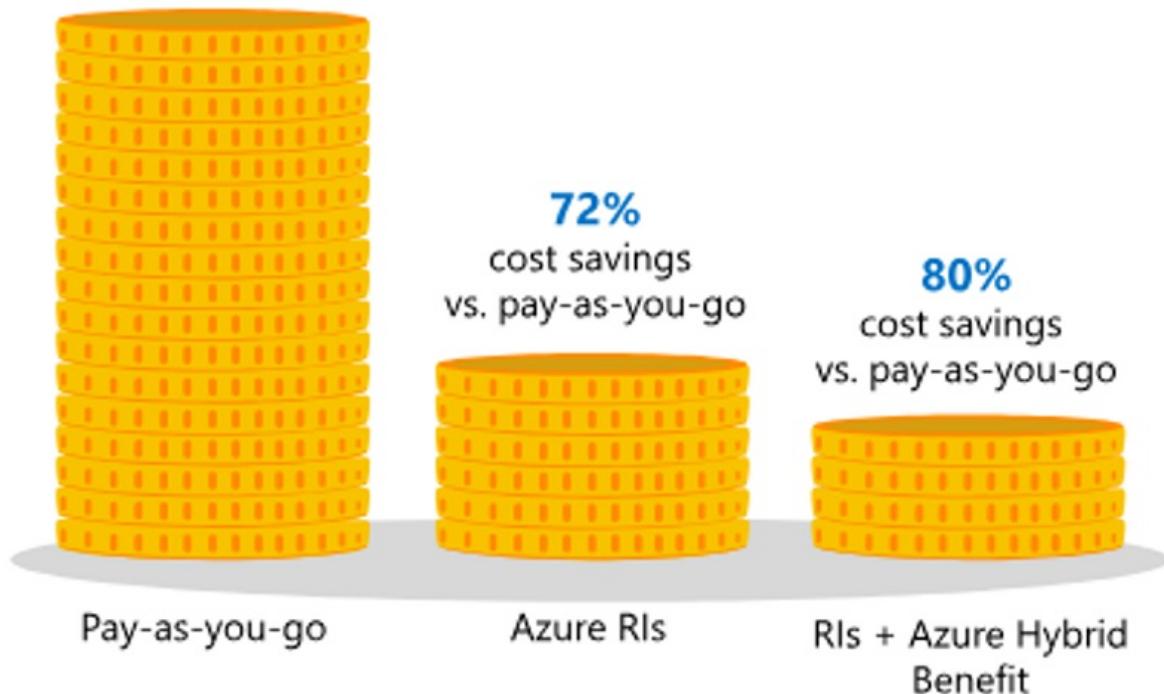


Figure 1: Azure reserved VMs.

## Learn more:

- Learn about [Azure Reservations](#).
- Read the [reserved instances FAQ](#).
- Review [pricing guidance for SQL Server Azure VMs](#).

## Best practice: Aggregate cloud spend across subscriptions

It's inevitable that eventually you'll have more than one Azure subscription. For example, you might need an additional subscription to separate development and production boundaries, or you might have a platform that requires a separate subscription for each client. Having the ability to aggregate data reporting across all the subscriptions into a single platform is a valuable feature.

To do this, you can use Azure Cost Management + Billing APIs. Then, after aggregating data into a single source such as Azure SQL Database, you can use tools like Power BI to surface the aggregated data. You can create aggregated subscription reports, and granular reports. For example, for users who need proactive insights into cost management, you can create specific views of costs, based on department, resource group, or other information. You don't need to provide them with full access to Azure billing data.

## Learn more:

- Read the [Azure Consumption APIs overview](#).
- Learn about [connecting to Azure Consumption Insights in Power BI Desktop](#).
- Learn to [manage access to billing information for Azure using role-based access control \(RBAC\)](#).

## Best practice: Monitor resource utilization

In Azure you pay for what you use, when resources are consumed, and you don't pay when they aren't. For VMs, billing occurs when a VM is allocated, and you aren't charged after a VM is deallocated. With this in mind you should monitor VMs in use, and verify VM sizing.

- Continually evaluate your VM workloads to determine baselines.
- For example, if your workload is used heavily Monday through Friday, 8am to 6pm, but hardly used outside those hours, you could downgrade VMs outside peak times. This might mean changing VM sizes, or using virtual machine scale sets to autoscale VMs up or down.
- Some companies "snooze" VMs by putting them on a calendar that specifies when they should be available, and when they're not needed.
- In addition to VM monitoring, you should monitor other networking resources such as ExpressRoute and virtual network gateways for under and over use.
- You can monitor VM usage using Microsoft tools such as Azure Cost Management + Billing, Azure Monitor, and Azure Advisor. Third-party tools are also available.

**Learn more:**

- Read overviews of [Azure Monitor](#) and [Azure Advisor](#).
- Get [Azure Advisor cost recommendations](#).
- Learn how to [optimize costs from recommendations](#), and [prevent unexpected charges](#).
- Learn about the [Azure resource optimization \(ARO\) toolkit](#).

## Best practice: Reduce nonproduction costs

Development, testing, and quality assurance (QA) environments are needed during development cycles. Unfortunately, it is common for those environments to stay provisioned long after they cease to be useful. A regular review of unused nonproduction environments can have an immediate impact on costs.

Additionally, consider general cost reductions for any nonproduction environments:

- Reduce nonproduction resources to use lower cost B-series VMs and standard storage.
- Reduce nonproduction compute costs by using Spot VMs.
- Apply Azure policies to require resource level cost-reductions for any nonproduction resources.

**Learn more:**

- [Use tags](#) to identify dev, test, or QA targets for resizing or termination.
- [Auto-shutdown VMs](#) sets a nightly termination time for VMs. Using this feature will stop nonproduction VMs each night, requiring developers to restart those VMs when they're ready to resume development.
- [Spot VMs](#) allows it to take advantage of unused Azure capacity at a significant cost savings. However, at any point in time when Azure needs the capacity back, the Azure infrastructure will evict Spot VMs.
- Encourage development teams to use [Azure DevTest Labs](#) to establish their own cost-control approaches and avoid impact of the standard auto-shutdown timing in the prior step.

## Best practice: Use Azure Cost Management + Billing

Microsoft provides Azure Cost Management + Billing to help you track spending:

- Helps you to monitor and control Azure spending, and optimize use of resources.
- Reviews your entire subscription and all of its resources, and makes recommendations.
- Provides a full API to integrate external tools and financial systems for reporting.
- Tracks resource usage and manage cloud costs with a single, unified view.
- Provides rich operational and financial insights to help you make informed decisions.

In Azure Cost Management + Billing, you can:

- **Create a budget:** Create a budget for financial accountability.
  - You can account for the services you consume or subscribe to for a specific period (monthly, quarterly, annually) and a scope (subscriptions/resource groups). For example, you can create an Azure subscription budget for a monthly, quarterly, or annual period.
  - After you create a budget, it's shown in cost analysis. Viewing your budget against current spending is one of the first steps needed when analyzing your costs and spending.
  - Email notifications can be sent when budget thresholds are reached.
  - You can export costs management data to Azure Storage, for analysis.

NAME	PERIOD	START DA...	END DA...	BUDGET	CURRENT COST	PROGRESS
FY19 Monthly	Monthly	7/1/2018	7/1/2028	\$4,500.00	\$3,508.34	77.96%
FY19 Quarterly	Quarterly	7/1/2018	7/1/2028	\$13,500.00	\$8,461.29	62.68%
FY19	Annually	7/1/2018	7/1/2028	\$54,000.00	\$8,461.29	15.67%

#### *Budgets in Azure Cost Management + Billing.*

- **Do a cost analysis:** Get a cost analysis to explore and analyze your organizational costs, to help you understand how costs are accrued, and identify spending trends.
  - Cost analysis is available to EA users.
  - You can view cost analysis data for various scopes, including by department, account, subscription, or resource group.
  - You can get a cost analysis that shows total costs for the current month, and accumulated daily costs.

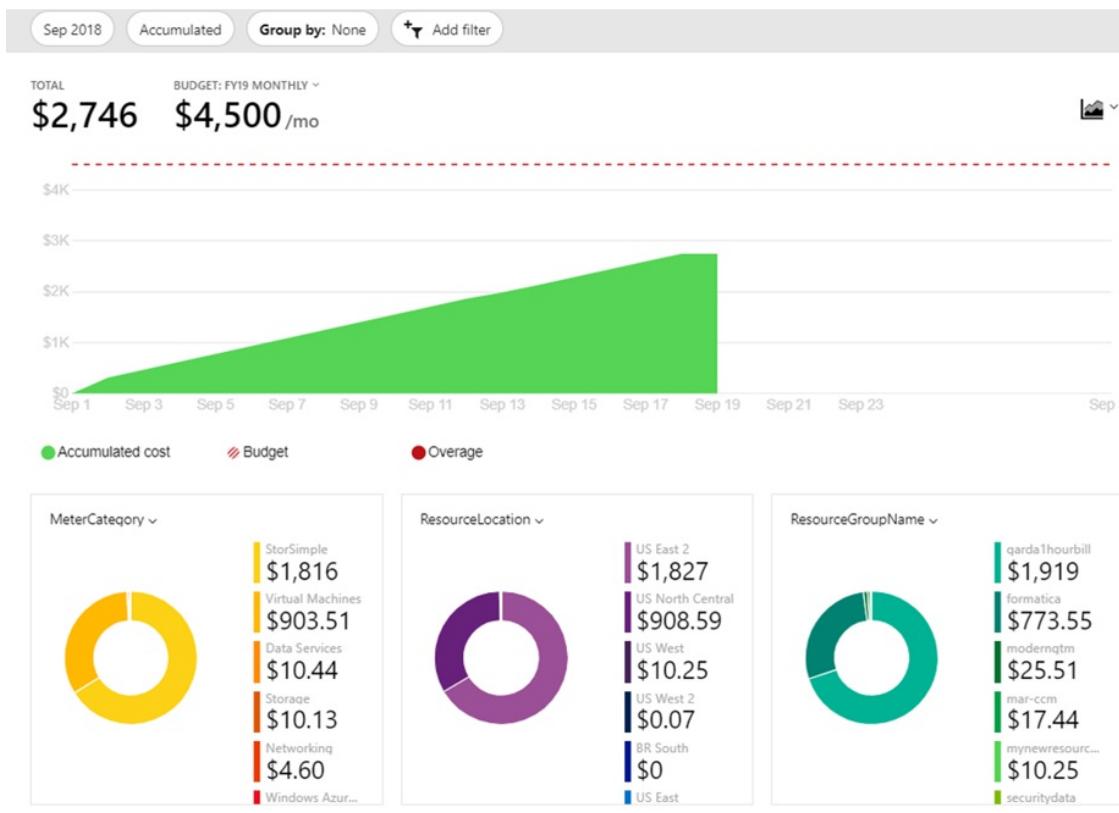


Figure: Azure Cost Management + Billing analysis.

- **Get recommendations:** Get Advisor recommendations that show you how you can optimize and improve efficiency.

#### Learn more:

- Read the [Azure Cost Management + Billing overview](#).
- Learn how to optimize your cloud investment with [Azure Cost Management + Billing](#).
- Learn how to use [Azure Cost Management + Billing reports](#).
- Review a tutorial on [optimizing costs from recommendations](#).
- Review the [Azure Consumption APIs](#).

## Best practice: Implement resource group budgets

Often, resource groups are used to represent cost boundaries. Together with this usage pattern, the Azure team continues to develop new and enhanced ways to track and analyze resource spending at different levels, including the ability to create budgets at the resource group and resources.

- A resource group budget helps you track the costs associated with a resource group.
- You can trigger alerts and run a wide variety of playbooks as the budget is reached or exceeded.

#### Learn more:

- Learn how to [manage costs with Azure budgets](#).
- Review a tutorial on [creating and managing an Azure budget](#).

## Best practice: Review Azure Advisor recommendations

Azure Advisor cost recommendations identify opportunities to reduce costs. When budgets appear high or utilization appears low, use this report to find immediate opportunities to quickly align costs.

#### Learn more:

- Review [Azure Advisor cost recommendations](#) to take immediate actions.

## Best practice: Optimize Azure Monitor retention

As you move resources into Azure and enable diagnostic logging for them, you generate a lot of log data. Typically this log data is sent to a storage account that's mapped to a Log Analytics workspace.

- The longer the log data retention period, the more data you'll have.
- Not all log data is equal, and some resources will generate more log data than others.
- Due to regulations and compliance, it's likely that you'll need to retain log data for some resources longer than others.
- Balance between optimizing your log storage costs and keeping the log data you need.
- We recommend evaluating and setting up the logging immediately after completing a migration, so that you aren't spending money retaining logs of no importance.

**Learn more:**

- Learn about [monitoring usage and estimated costs](#).

## Best practice: Optimize storage

If you followed best practices for selecting storage before adoption, you're probably reaping some benefits. You can probably optimize some additional storage costs. Over time, blobs and files become stale. Data might not be used anymore, but regulatory requirements might mean that you need to keep it for a certain period. As such, you might not need to store it on the high-performance storage that you used for the original adoption.

Identifying and moving stale data to cheaper storage areas can have a huge impact on your monthly storage budget and cost savings. Azure provides many ways to help you identify and then store this stale data.

- Take advantage of access tiers for general-purpose v2 storage by moving less important data from hot to cool and archived tiers.
- Use StorSimple to help move stale data based on customized policies.

**Learn more:**

- Learn more about [access tiers](#).
- Read the [StorSimple overview](#).
- Review [StorSimple pricing](#).

## Best practice: Automate VM optimization

The ultimate goal of running a VM in the cloud is to maximize the CPU, memory, and disk that it uses. If you discover VMs that aren't optimized, or have frequent periods when VMs aren't used, it makes sense to either shut them down, or downscale them using virtual machine scale sets.

You can optimize a VM with Azure Automation, virtual machine scale sets, auto-shutdown, and scripted or third-party solutions.

**Learn more:**

- Learn about [vertical autoscaling](#).
- Review [Azure DevTest Labs: schedule VM auto-start](#).
- Learn how to [start or stop VMs off hours in Azure Automation](#).
- Get more information about [Azure Advisor](#), and the [Azure resource optimization \(ARO\) toolkit](#).

# Best practice: Use Logic Apps and runbooks with Budgets API

Azure provides a REST API that can access your tenant billing information.

- You can use the Budgets API to integrate external systems and workflows that are triggered by metrics that you build from the API data.
- You can pull usage and resource data into your preferred data analysis tools.
- The Azure Resource Usage API and the Azure Resource RateCard API can help you accurately predict and manage your costs.
- The APIs are implemented as a resource provider and are included in the APIs exposed by Azure Resource Manager.
- The Budgets API can be integrated with Azure Logic Apps and Azure Automation runbooks.

**Learn more:**

- Learn more about the [Budgets API](#).
- [Get insights](#) into Azure usage with the Azure Billing APIs.

## Next steps

With an understanding of best practices, examine the [Cost Management toolchain](#) to identify Azure tools and features to help you execute these best practices.

[Cost Management toolchain for Azure](#)

# Cost Management tools in Azure

11/9/2020 • 2 minutes to read • [Edit Online](#)

The [Cost Management discipline](#) is one of the [Five Disciplines of Cloud Governance](#). This discipline focuses on ways of establishing cloud spending plans, allocating cloud budgets, monitoring and enforcing cloud budgets, detecting costly anomalies, and adjusting the cloud governance plan when actual spending is misaligned.

The following is a list of Azure native tools that can help mature the policies and processes that support this discipline.

TOOL	AZURE PORTAL	AZURE COST MANAGEMENT + BILLING	POWER BI DESKTOP CONNECTOR	AZURE POLICY
Budget control	No	Yes	No	Yes
Monitor spending on single resource	Yes	Yes	Yes	No
Monitor spending across multiple resources	No	Yes	Yes	No
Control spending on single resource	Yes, manual sizing	Yes	No	Yes
Enforce spending across multiple resources	No	Yes	No	Yes
Enforce accounting metadata on resources	No	No	No	Yes
Monitor and detect trends	Yes	Yes	Yes	No
Detect spending anomalies	No	Yes	Yes	No
Socialize deviations	No	Yes	Yes	No

# Security Baseline discipline overview

11/9/2020 • 2 minutes to read • [Edit Online](#)

Security baseline is one of the [Five Disciplines of Cloud Governance](#) within the [Cloud Adoption Framework governance model](#). Security is a component of any IT deployment, and the cloud introduces unique security concerns. Many businesses are subject to regulatory requirements that make protecting sensitive data a major organizational priority when considering a cloud transformation. Identifying potential security threats to your cloud environment and establishing processes and procedures for addressing these threats should be a priority for any IT security or cybersecurity team. The Security Baseline discipline ensures technical requirements and security constraints are consistently applied to cloud environments, as those requirements mature.

## NOTE

Security Baseline discipline does not replace the existing IT teams, processes, and procedures that your organization uses to secure cloud-deployed resources. The primary purpose of this discipline is to identify security-related business risks and provide risk-mitigation guidance to the IT staff responsible for security infrastructure. As you develop governance policies and processes make sure to involve relevant IT teams in your planning and review processes.

This article outlines the approach to developing a Security Baseline discipline as part of your cloud governance strategy. The primary audience for this guidance is your organization's cloud architects and other members of your cloud governance team. The decisions, policies, and processes that emerge from this discipline should involve engagement and discussions with relevant members of your IT and security teams, especially those technical leaders responsible for implementing networking, encryption, and identity services.

Making the correct security decisions is critical to the success of your cloud deployments and wider business success. If your organization lacks in-house expertise in cybersecurity, consider engaging external security consultants as a component of this discipline. Also consider engaging [Microsoft Consulting Services](#), the [Microsoft FastTrack](#) cloud adoption service, or other external cloud adoption experts to discuss concerns related to this discipline.

## Policy statements

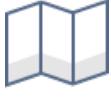
Actionable policy statements and the resulting architecture requirements serve as the foundation of a Security Baseline discipline. Use [sample policy statements](#) as a starting point for defining your Security Baseline policies.

### Caution

The sample policies come from common customer experiences. To better align these policies to specific cloud governance needs, execute the following steps to create policy statements that meet your unique business needs.

## Develop governance policy statements

The following steps offer examples and potential options to consider when developing your Security Baseline discipline. Use each step as a starting point for discussions within your cloud governance team and with affected business, IT, and security teams across your organization to establish the policies and processes needed to manage security-related risks.

	<p><a href="#">Security Baseline discipline template</a>: Download the template for documenting a Security Baseline discipline.</p>
	<p><a href="#">Business risks</a>: Understand the motives and risks commonly associated with the Security Baseline discipline.</p>
	<p><a href="#">Indicators and metrics</a>: Indicators to understand whether it is the right time to invest in the Security Baseline discipline.</p>
	<p><a href="#">Policy adherence processes</a>: Suggested processes for supporting policy compliance in the Security Baseline discipline.</p>
	<p><a href="#">Maturity</a>: Align cloud management maturity with phases of cloud adoption.</p>
	<p><a href="#">Toolchain</a>: Azure services that can be implemented to support the Security Baseline discipline.</p>

## Next steps

Get started by evaluating business risks in a specific environment.

[Understand business risks](#)

# Security Baseline discipline template

11/9/2020 • 2 minutes to read • [Edit Online](#)

The first step to implementing change is communicating what is desired. The same is true when changing governance practices. The template below provides a starting point for documenting and communicating policy statements that govern security related issues in the cloud.

As your discussions progress, use this template's structure as a model for capturing the business risks, risk tolerances, compliance processes, and tooling needed to define your organization's Security Baseline policy statements.

## IMPORTANT

This template is a limited sample. Before updating this template to reflect your requirements, you should review the subsequent steps for defining an effective Security Baseline discipline within your cloud governance strategy.

[Download the Security Baseline discipline template](#)

## Next steps

Solid governance practices start with an understanding of business risk. Review the article on business risks and begin to document the business risks that align with your current cloud adoption plan.

[Understand business risks](#)

# Motivations and business risks in the Security Baseline discipline

11/9/2020 • 2 minutes to read • [Edit Online](#)

This article discusses the reasons that customers typically adopt a Security Baseline discipline within a cloud governance strategy. It also provides a few examples of potential business risks that can drive policy statements.

## Relevance

Security is a key concern for any IT organization. Cloud deployments face many of the same security risks as workloads hosted in traditional on-premises datacenters. The nature of public cloud platforms, with a lack of direct ownership of the physical hardware storing and running your workloads, means cloud security requires its own policy and processes.

One of the primary things that sets cloud security governance apart from traditional security policy is the ease with which resources can be created, potentially adding vulnerabilities if security isn't considered before deployment. The flexibility that technologies like [Software Defined Networking \(SDN\)](#) provide for rapidly changing your cloud-based network topology can also easily modify your overall network attack surface in unforeseen ways. Cloud platforms also provide tools and features that can improve your security capabilities in ways not always possible in on-premises environments.

The amount you invest into security policy and processes will depend a great deal on the nature of your cloud deployment. Initial test deployments may only need the most basic of security policies in place, while a mission-critical workload will entail addressing complex and extensive security needs. All deployments will need to engage with the discipline at some level.

The Security Baseline discipline covers the corporate policies and manual processes that you can put in place to protect your cloud deployment against security risks.

### NOTE

While it's important to understand the [Identity Baseline discipline](#) in the context of the Security Baseline discipline and how that relates to access control, the [Five Disciplines of Cloud Governance](#) treats it as a separate discipline.

## Business risk

The Security Baseline discipline attempts to address core security-related business risks. Work with your business to identify these risks and monitor each of them for relevance as you plan for and implement your cloud deployments.

Risks differ between organizations. Use this list of common security-related risks as a starting point for discussions within your cloud governance team:

- **Data breach:** Inadvertent exposure or loss of sensitive cloud-hosted data can lead to losing customers, contractual issues, or legal consequences.
- **Service disruption:** Outages and other performance issues due to insecure infrastructure interrupts normal operations and can result in lost productivity or lost business.

## Next steps

Use the [Security Baseline discipline template](#) to document business risks that are likely to be introduced by the current cloud adoption plan.

Once an understanding of realistic business risks is established, the next step is to document the business's tolerance for risk and the indicators and key metrics to monitor that tolerance.

[Understand indicators, metrics, and risk tolerance](#)

# Risk tolerance metrics and indicators in the Security Baseline discipline

11/9/2020 • 4 minutes to read • [Edit Online](#)

Learn to quantify business risk tolerance associated with the Security Baseline discipline. Defining metrics and indicators helps to create a business case for investing in the maturity of this discipline.

## Metrics

The Security Baseline discipline generally focuses on identifying potential vulnerabilities in your cloud deployments. As part of your risk analysis you'll want to gather data related to your security environment to determine how much risk you face, and how important investment in your Security Baseline discipline is for your planned cloud deployments.

Every organization has different security environments and requirements and different potential sources of security data. The following are examples of useful metrics that you should gather to help evaluate risk tolerance within the Security Baseline discipline:

- **Data classification:** Number of cloud-stored data and services that are unclassified according to on your organization's privacy, compliance, or business impact standards.
- **Number of sensitive data stores:** Number of storage endpoints or databases that contain sensitive data and should be protected.
- **Number of unencrypted data stores:** Number of sensitive data stores that are not encrypted.
- **Attack surface:** How many total data sources, services, and applications will be cloud-hosted. What percentage of these data sources are classified as sensitive? What percentage of these applications and services are mission-critical?
- **Covered standards:** Number of security standards defined by the security team.
- **Covered resources:** Deployed assets that are covered by security standards.
- **Overall standards compliance:** Ratio of compliance adherence to security standards.
- **Attacks by severity:** How many coordinated attempts to disrupt your cloud-hosted services, such as through distributed denial of service (DDoS) attacks, does your infrastructure experience? What is the size and severity of these attacks?
- **Malware protection:** Percentage of deployed virtual machines (VMs) that have all required anti-malware, firewall, or other security software installed.
- **Patch latency:** How long has it been since VMs have had OS and software patches applied.
- **Security health recommendations:** Number of security software recommendations for resolving health standards for deployed resources, organized by severity.

## Risk tolerance indicators

Cloud platforms provide a baseline set of features that enable small deployment teams to configure basic security settings without extensive additional planning. As a result, small dev/test or experimental first workloads that do not include sensitive data represent a relatively low level of risk, and will likely not need much in the way of formal Security Baseline policy. As soon as important data or mission-critical functionality is moved to the cloud, security risks increase, while tolerance for those risks diminishes rapidly. As more of your data and functionality is deployed to the cloud, the more likely you need an increased investment in the Security Baseline discipline.

In the early stages of cloud adoption, work with your IT security team and business stakeholders to identify

[business risks](#) related to security, then determine an acceptable baseline for security risk tolerance. This section of the Cloud Adoption Framework provides examples, but the detailed risks and baselines for your company or deployments may be different.

Once you have a baseline, establish minimum benchmarks representing an unacceptable increase in your identified risks. These benchmarks act as triggers for when you need to take action to remediate these risks. The following are a few examples of how security metrics, such as those discussed above, can justify an increased investment in the Security Baseline discipline.

- **Mission-critical workloads trigger.** A company deploying mission-critical workloads to the cloud should invest in the Security Baseline discipline to prevent potential disruption of service or sensitive data exposure.
- **Protected data trigger.** A company hosting data on the cloud that can be classified as confidential, private, or otherwise subject to regulatory concerns. They need a Security Baseline discipline to ensure that this data is not subject to loss, exposure, or theft.
- **External attacks trigger.** A company that experiences serious attacks against their network infrastructure  $x$  times per month could benefit from the Security Baseline discipline.
- **Standards compliance trigger.** A company with more than  $x\%$  of resources out of security standards compliance should invest in the Security Baseline discipline to ensure standards are applied consistently across your IT infrastructure.
- **Cloud estate size trigger.** A company hosting more than  $x$  applications, services, or data sources. Large cloud deployments can benefit from investment in the Security Baseline discipline to ensure that their overall attack surface is properly protected against unauthorized access or other external threats.
- **Security software compliance trigger.** A company where less than  $x\%$  of deployed virtual machines have all required security software installed. A Security Baseline discipline can be used to ensure software is installed consistently on all software.
- **Patching trigger.** A company where deployed virtual machines or services where OS or software patches have not been applied in the last  $x$  days. A Security Baseline discipline can be used to ensure patching is kept up-to-date within a required schedule.
- **Security-focused.** Some companies will have strong security and data confidentiality requirements even for test and experimental workloads. These companies will need to invest in the Security Baseline discipline before any deployments can begin.

The exact metrics and triggers you use to gauge risk tolerance and the level of investment in the Security Baseline discipline will be specific to your organization, but the examples above should serve as a useful base for discussion within your cloud governance team.

## Next steps

Use the [Security Baseline discipline template](#) to document metrics and tolerance indicators that align to the current cloud adoption plan.

Review sample Security Baseline policies as a starting point to develop your own policies to address specific business risks aligned with your cloud adoption plans.

[Review sample policies](#)

# Security Baseline sample policy statements

11/9/2020 • 4 minutes to read • [Edit Online](#)

Individual cloud policy statements are guidelines for addressing specific risks identified during your risk assessment process. These statements should provide a concise summary of risks and plans to deal with them. Each statement definition should include these pieces of information:

- **Technical risk:** A summary of the risk this policy will address.
- **Policy statement:** A clear summary explanation of the policy requirements.
- **Technical options:** Actionable recommendations, specifications, or other guidance that IT teams and developers can use when implementing the policy.

The following sample policy statements address common security-related business risks. These statements are examples you can reference when drafting policy statements to address your organization's needs. These examples are not meant to be prescriptive, and there are potentially several policy options for dealing with each identified risk. Work closely with business, security, and IT teams to identify the best policies for your unique set of risks.

## Asset classification

**Technical risk:** Assets that are not correctly identified as mission-critical or involving sensitive data may not receive sufficient protections, leading to potential data leaks or business disruptions.

**Policy statement:** All deployed assets must be categorized by criticality and data classification. Classifications must be reviewed by the cloud governance team and the application owner before deployment to the cloud.

**Potential design option:** Establish [resource tagging standards](#) and ensure IT staff apply them consistently to any deployed resources using [Azure resource tags](#).

## Data encryption

**Technical risk:** There is a risk of protected data being exposed during storage.

**Policy statement:** All protected data must be encrypted when at rest.

**Potential design option:** See the [Azure encryption overview](#) article for a discussion of how data at rest encryption is performed on the Azure platform. Additional controls such as in account data encryption and control over how storage account settings can be changed should also be considered.

## Network isolation

**Technical risk:** Connectivity between networks and subnets within networks introduces potential vulnerabilities that can result in data leaks or disruption of mission-critical services.

**Policy statement:** Network subnets containing protected data must be isolated from any other subnets. Network traffic between protected data subnets is to be audited regularly.

**Potential design option:** In Azure, network and subnet isolation is managed through [Azure Virtual Network](#).

## Secure external access

**Technical risk:** Allowing access to workloads from the public internet introduces a risk of intrusion resulting in unauthorized data exposure or business disruption.

**Policy statement:** No subnet containing protected data can be directly accessed over public internet or across datacenters. Access to those subnets must be routed through intermediate subnets. All access into those subnets must come through a firewall solution capable of performing packet scanning and blocking functions.

**Potential design option:** In Azure, secure public endpoints by deploying a [perimeter network between the public internet and your cloud-based network](#). Consider deployment, configuration, and automation of [Azure Firewall](#).

## DDoS protection

**Technical risk:** Distributed denial of service (DDoS) attacks can result in a business interruption.

**Policy statement:** Deploy automated DDoS mitigation mechanisms to all publicly accessible network endpoints. No public-facing web site backed by IaaS should be exposed to the internet without DDoS.

**Potential design option:** Use [Azure DDoS Protection Standard](#) to minimize disruptions caused by DDoS attacks.

## Secure on-premises connectivity

**Technical risk:** Unencrypted traffic between your cloud network and on-premises over the public internet is vulnerable to interception, introducing the risk of data exposure.

**Policy statement:** All connections between the on-premises and cloud networks must take place either through a secure encrypted VPN connection or a dedicated private WAN link.

**Potential design option:** In Azure, use ExpressRoute or Azure VPN to establish private connections between your on-premises and cloud networks.

## Network monitoring and enforcement

**Technical risk:** Changes to network configuration can lead to new vulnerabilities and data exposure risks.

**Policy statement:** Governance tooling must audit and enforce network configuration requirements defined by the security baseline team.

**Potential design option:** In Azure, network activity can be monitored using [Azure Network Watcher](#), and [Azure Security Center](#) can help identify security vulnerabilities. Azure Policy allows you to restrict network resources and resource configuration policy according to limits defined by the security team.

## Security review

**Technical risk:** Over time, new security threats and attack types emerge, increasing the risk of exposure or disruption of your cloud resources.

**Policy statement:** Trends and potential exploits that could affect cloud deployments should be reviewed regularly by the security team to provide updates to Security Baseline tools used in the cloud.

**Potential design option:** Establish a regular security review meeting that includes relevant IT and governance team members. Review existing security data and metrics to establish gaps in current policy and Security Baseline tools, and update policy to remediate any new risks. Use [Azure Advisor](#) and [Azure Security Center](#) to gain actionable insights on emerging threats specific to your deployments.

## Next steps

Use the samples mentioned in this article as a starting point to develop policies that address specific security risks that align with your cloud adoption plans.

To begin developing your own custom Security Baseline policy statements, download the [Security Baseline](#)

[discipline template](#).

To accelerate adoption of this discipline, choose the [actionable governance guide](#) that most closely aligns with your environment. Then modify the design to incorporate your specific corporate policy decisions.

Building on risks and tolerance, establish a process for governing and communicating Security Baseline policy adherence.

[Establish policy compliance processes](#)

# Security Baseline policy compliance processes

11/9/2020 • 5 minutes to read • [Edit Online](#)

This article discusses an approach to policy adherence processes that govern the [Security Baseline discipline](#). Effective governance of cloud security starts with recurring manual processes designed to detect vulnerabilities and impose policies to remediate those security risks. This requires regular involvement of the cloud governance team and interested business and IT stakeholders to review and update policy and ensure policy compliance. In addition, many ongoing monitoring and enforcement processes can be automated or supplemented with tooling to reduce the overhead of governance and allow for faster response to policy deviation.

## Planning, review, and reporting processes

The best Security Baseline tools in the cloud are only as good as the processes and policies that they support. The following is a set of example processes commonly involved in the Security Baseline discipline. Use these examples as a starting point when planning the processes that will allow you to continue to update security policy based on business change and feedback from the security and IT teams tasked with turning governance guidance into action.

**Initial risk assessment and planning:** As part of your initial adoption of the Security Baseline discipline, identify your core business risks and tolerances related to cloud security. Use this information to discuss specific technical risks with members of your IT and security teams and develop a baseline set of security policies for mitigating these risks to establish your initial governance strategy.

**Deployment planning:** Before deploying any workload or asset, perform a security review to identify any new risks and ensure all access and data security policy requirements are met.

**Deployment testing:** As part of the deployment process for any workload or asset, the cloud governance team, in cooperation with your corporate security teams, will be responsible for reviewing the deployment to validate security policy compliance.

**Annual planning:** On an annual basis, perform a high-level review of Security Baseline strategy. Explore future corporate priorities and updated cloud adoption strategies to identify potential risk increase and other emerging security needs. Also use this time to review the latest security baseline best practices and integrate these into your policies and review processes.

**Quarterly review and planning:** On a quarterly basis perform a review of security audit data and incident reports to identify any changes required in security policy. As part of this process, review the current cybersecurity landscape to proactively anticipate emerging threats, and update policy as appropriate. After the review is complete, align design guidance with updated policy.

This planning process is also a good time to evaluate the current membership of your cloud governance team for knowledge gaps related to new or changing policy and risks related to security. Invite relevant IT staff to participate in reviews and planning as either temporary technical advisors or permanent members of your team.

**Education and training:** On a bimonthly basis, offer training sessions to make sure IT staff and developers are up-to-date on the latest security policy requirements. As part of this process review and update any documentation, guidance, or other training assets to ensure they're in sync with the latest corporate policy statements.

**Monthly audit and reporting reviews:** On a monthly basis, perform an audit on all cloud deployments to assure their continued alignment with security policy. Review security related activities with IT staff and identify any compliance issues not already handled as part of the ongoing monitoring and enforcement process. The result

of this review is a report for the cloud strategy team and each cloud adoption team to communicate overall adherence to policy. The report is also stored for auditing and legal purposes.

## Processes for ongoing monitoring

A successful Security Baseline strategy is successful depends on visibility into the current and past state of your cloud infrastructure. Without the ability to analyze the relevant metrics and data of your cloud resources security health and activity, you cannot identify changes in your risks or detect violations of your risk tolerances. The ongoing governance processes discussed above require quality data to ensure policy can be modified to better protect your infrastructure against changing threats and security requirements.

Ensure that your security and IT teams have implemented automated monitoring systems for your cloud infrastructure that capture the relevant logs data you need to evaluate risk. Be proactive in monitoring these systems to ensure prompt detection and mitigation of potential policy violation, and ensure your monitoring strategy is in line with security needs.

## Violation triggers and enforcement actions

Because security noncompliance can lead to critical and data exposure and service disruption risks, the cloud governance team should have visibility into serious policy violations. Ensure IT staff have clear escalation paths for reporting security issues to the governance team members best suited to identify and verify that policy issues are mitigated.

When violations are detected, you should take actions to realign with policy as soon as possible. Your IT team can automate most violation triggers using the tools outlined in the [Security Baseline toolchain for Azure](#).

The following triggers and enforcement actions provide examples you can reference when planning how to use monitoring data to resolve policy violations:

- **Increase in attacks detected.** If any resource experiences a 25% increase in brute force or DDoS attacks, discuss with IT security staff and workload owner to determine remedies. Track issue and update guidance if policy revision is necessary to prevent future incidents.
- **Unclassified data detected.** Any data source without an appropriate privacy, security, or business impact classification will have external access denied until the classification is applied by the data owner and the appropriate level of data protection applied.
- **Security health issue detected.** Disable access to any virtual machines (VMs) that have known access or malware vulnerabilities identified until appropriate patches or security software can be installed. Update policy guidance to account for any newly detected threats.
- **Network vulnerability detected.** Access to any resource not explicitly allowed by the network access policies should trigger an alert to IT security staff and the relevant workload owner. Track issue and update guidance if policy revision is necessary to mitigate future incidents.

## Next steps

Use the [Security Baseline discipline template](#) to document the processes and triggers that align to the current cloud adoption plan.

For guidance on executing cloud management policies in alignment with adoption plans, see the article on discipline improvement.

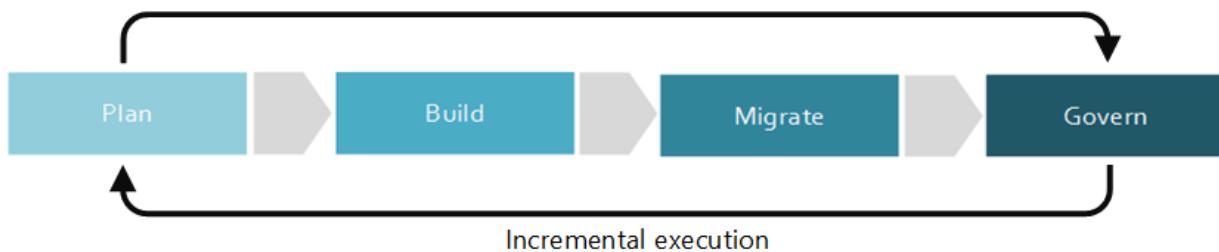
[Security Baseline discipline improvement](#)

# Security Baseline discipline improvement

11/9/2020 • 5 minutes to read • [Edit Online](#)

The Security Baseline discipline focuses on ways of establishing policies that protect the network, assets, and most importantly the data that will reside on a cloud provider's solution. Within the Five Disciplines of Cloud Governance, the Security Baseline discipline includes classification of the digital estate and data. It also includes documentation of risks, business tolerance, and mitigation strategies associated with the security of the data, assets, and network. From a technical perspective, this also includes involvement in decisions regarding [encryption](#), [network requirements](#), [hybrid identity strategies](#), and the [processes](#) used to develop Security Baseline policies for the cloud.

This article outlines some potential tasks your company can engage in to better develop and mature the Security Baseline discipline. These tasks can be broken down into planning, building, adopting, and operating phases of implementing a cloud solution, which are then iterated on allowing the development of an [incremental approach to cloud governance](#).



*Figure 1: Phases of an incremental approach to cloud governance.*

It's impossible for any one document to account for the requirements of all businesses. As such, this article outlines suggested minimum and potential example activities for each phase of the governance maturation process. The initial objective of these activities is to help you build a [policy MVP](#) and establish a framework for incremental policy improvement. Your cloud governance team will need to decide how much to invest in these activities to improve your Security Baseline discipline.

#### Caution

Neither the minimum or potential activities outlined in this article are aligned to specific corporate policies or third-party compliance requirements. This guidance is designed to help facilitate the conversations that will lead to alignment of both requirements with a cloud governance model.

## Planning and readiness

This phase of governance maturity bridges the divide between business outcomes and actionable strategies. During this process, the leadership team defines specific metrics, maps those metrics to the digital estate, and begins planning the overall migration effort.

#### Minimum suggested activities:

- Evaluate your [Security Baseline toolchain](#) options.
- Develop a draft architecture guidelines document and distribute to key stakeholders.
- Educate and involve the people and teams affected by the development of architecture guidelines.
- Add prioritized security tasks to your migration backlog.

#### Potential activities:

- Define a data classification schema.
- Conduct a digital estate planning process to inventory the current IT assets powering your business processes and supporting operations.
- Conduct a [policy review](#) to begin the process of modernizing existing corporate IT security policies, and define MVP policies addressing known risks.
- Review your cloud platform's security guidelines. For Azure these can be found in the [Microsoft Service Trust Portal](#).
- Determine whether your Security Baseline policy includes a [security development lifecycle](#).
- Evaluate network, data, and asset-related business risks based on the next one to three releases, and gauge your organization's tolerance for those risks.
- Review Microsoft's [top trends in cybersecurity](#) report for an overview of the current security landscape.
- Consider developing a [DevSecOps](#) role in your organization.

## Build and predeployment

Several technical and nontechnical prerequisites are required to successfully migrate an environment. This process focuses on the decisions, readiness, and core infrastructure that proceeds a migration.

### Minimum suggested activities:

- Implement your [Security Baseline toolchain](#) by rolling out in a predeployment phase.
- Update the architecture guidelines document and distribute to key stakeholders.
- Implement security tasks on your prioritized migration backlog.
- Develop educational materials and documentation, awareness communications, incentives, and other programs to help drive user adoption.

### Potential activities:

- Determine your organization's [encryption](#) strategy for cloud-hosted data.
- Evaluate your cloud deployment's [identity](#) strategy. Determine how your cloud-based identity solution will coexist or integrate with on-premises identity providers.
- Determine network boundary policies for your [Software Defined Networking \(SDN\)](#) design to ensure secure virtualized networking capabilities.
- Evaluate your organization's [least-privilege access](#) policies, and use task-based roles to provide access to specific resources.
- Apply security and monitoring mechanisms to all cloud services and virtual machines.
- Automate [security policies](#) where possible.
- Review your Security Baseline policy and determine whether you need to modify your plans according to best practices guidance such as those outlined in the [security development lifecycle](#).

## Adopt and migrate

Migration is an incremental process that focuses on the movement, testing, and adoption of applications or workloads in an existing digital estate.

### Minimum suggested activities:

- Migrate your [Security Baseline toolchain](#) from predeployment to production.
- Update the architecture guidelines document and distribute to key stakeholders.
- Develop educational materials and documentation, awareness communications, incentives, and other programs to help drive user adoption.

### Potential activities:

- Review the latest security baseline and threat information to identify any new business risks.
- Gauge your organization's tolerance to handle new security risks that may arise.
- Identify deviations from policy, and enforce corrections.
- Adjust security and access control automation to ensure maximum policy compliance.
- Validate that the best practices defined during the build and predeployment phases are properly executed.
- Review your least-privilege access policies and adjust access controls to maximize security.
- Test your Security Baseline toolchain against your workloads to identify and resolve any vulnerabilities.

## Operate and post-implementation

Once the transformation is complete, governance and operations must live on for the natural lifecycle of an application or workload. This phase of governance maturity focuses on the activities that commonly come after the solution is implemented and the transformation cycle begins to stabilize.

### Minimum suggested activities:

- Validate and refine your [Security Baseline toolchain](#).
- Customize notifications and reports to alert you of potential security issues.
- Refine the architecture guidelines to guide future adoption processes.
- Communicate and educate the affected teams periodically to ensure ongoing adherence to architecture guidelines.

### Potential activities:

- Discover patterns and behavior for your workloads and configure your monitoring and reporting tools to identify and notify you of any abnormal activity, access, or resource usage.
- Continuously update your monitoring and reporting policies to detect the latest vulnerabilities, exploits, and attacks.
- Have procedures in place to quickly stop unauthorized access and disable resources that may have been compromised by an attacker.
- Regularly review the latest security best practices and apply recommendations to your security policy, automation, and monitoring capabilities where possible.

## Next steps

Now that you understand the concept of cloud security governance, move on to learn more about [what security and best practices guidance Microsoft provides](#) for Azure.

[Learn about security guidance for Azure](#) [Introduction to Azure security](#) [Learn about logging, reporting, and monitoring](#)

# Cloud-native Security Baseline policy

11/9/2020 • 6 minutes to read • [Edit Online](#)

The [Security Baseline discipline](#) is one of the [Five Disciplines of Cloud Governance](#). This discipline focuses on general security topics including protection of the network, digital assets, and data. As outlined in the [policy review guide](#), the Cloud Adoption Framework includes three levels of sample policy: cloud-native, enterprise, and cloud-design-principle-compliant for each of the disciplines. This article discusses the cloud-native sample policy for the Security Baseline discipline.

## NOTE

Microsoft is in no position to dictate corporate or IT policy. This article will help you prepare for an internal policy review. It is assumed that this sample policy will be extended, validated, and tested against your corporate policy before attempting to use it. Any use of this sample policy as-is is discouraged.

## Policy alignment

This sample policy synthesizes a cloud-native scenario, meaning that the tools and platforms provided by Azure are sufficient to manage business risks involved in a deployment. In this scenario, it is assumed that a simple configuration of the default Azure services provides sufficient asset protection.

## Cloud security and compliance

Security is integrated into every aspect of Azure, offering unique security advantages derived from global security intelligence, sophisticated customer-facing controls, and a secure, hardened infrastructure. This powerful combination helps protect your applications and data, support your compliance efforts, and provide cost-effective security for organizations of all sizes. This approach creates a strong starting position for any security policy, but does not negate the need for equally strong security practices related to the security services being used.

### Built-in security controls

It's hard to maintain a strong security infrastructure when security controls are not intuitive and need to be configured separately. Azure includes built-in security controls across a variety of services that help you protect data and workloads quickly and manage risk across hybrid environments. Integrated partner solutions also let you easily transition existing protections to the cloud.

### Cloud-native identity policies

Identity is becoming the new boundary control plane for security, taking over that role from the traditional network-centric perspective. Network perimeters have become increasingly porous and that perimeter defense cannot be as effective as it was before the advent of bring your own device (BYOD) and cloud applications. Azure identity management and access control enable seamless secure access to all your applications.

A sample cloud-native policy for identity across cloud and on-premises directories, could include requirements like the following:

- Authorized access to resources with role-based access control (RBAC), multi-factor authentication, and single sign-on (SSO).
- Quick mitigation of user identities suspected of compromise.
- Just-in-time (JIT), just-enough access granted on a task-by-task basis to limit exposure of overprivileged admin credentials.

- Extended user identity and access to policies across multiple environments through Azure Active Directory.

While it is important to understand the [Identity Baseline discipline](#) in the context of the Security Baseline discipline, the [Five Disciplines of Cloud Governance](#) treats it as a separate discipline.

## **Network access policies**

Network control includes the configuration, management, and securing of network elements such as virtual networking, load balancing, DNS, and gateways. The controls provide a means for services to communicate and interoperate. Azure includes a robust and secure networking infrastructure to support your application and service connectivity requirements. Network connectivity is possible between resources located in Azure, between on-premises and Azure hosted resources, and to and from the internet and Azure.

A cloud-native policy for network controls may include requirements like the following:

- Hybrid connections to on-premises resources, might not be allowed in a cloud-native policy. Should a hybrid connection prove necessary, a more robust enterprise security policy sample would be a more relevant reference.
- Users can establish secure connections to and within Azure using virtual networks and network security groups.
- The native Windows Azure Firewall protects hosts from malicious network traffic by limiting port access. A good example of this policy is a requirement to block or not enable traffic directly to a VM over SSH/RDP.
- Services like the Azure Web Application Firewall (WAF) on Azure Application Gateway and Azure DDoS protection safeguard applications and ensure availability for virtual machines running in Azure. These features should not be disabled.

## **Data protection**

One of the keys to data protection in the cloud is accounting for the possible states in which your data may occur, and what controls are available for each state. For the purpose of Azure data security and encryption best practices, recommendations focus on the following data states:

- Data encryption controls are built into services from virtual machines to storage and SQL Database.
- As data moves between clouds and customers, it can be protected using industry-standard encryption protocols.
- Azure Key Vault enables users to safeguard and control cryptographic keys, passwords, connection strings and certificates used by cloud applications and services.
- Azure Information Protection will help classify, label, and protect your sensitive data within applications.

While these features are built into Azure, each of the above requires configuration and could increase costs.

Alignment of each cloud-native feature with a [data classification strategy](#) is highly suggested.

## **Security monitoring**

Security monitoring is a proactive strategy that audits your resources to identify systems that do not meet organizational standards or best practices. Azure Security Center provides unified security baseline and Azure Advanced Threat Protection across hybrid cloud workloads. With Security Center, you can apply security policies across your workloads, limit your exposure to threats, and detect and respond to attacks, including:

- Unified view of security across all on-premises and cloud workloads with Azure Security Center.
- Continuous monitoring and security assessments to ensure compliance and remediate any vulnerabilities.
- Interactive tools and contextual threat intelligence for streamlined investigation.
- Extensive logging and integration with existing security information.
- Reduces the need for expensive, nonintegrated, one off security solutions.

## **Extend cloud-native policies**

Using the cloud can reduce some of the security burden. Microsoft provides physical security for Azure datacenters and helps protect the cloud platform against infrastructure threats such as a DDoS attack. Given that Microsoft has

thousands of cybersecurity specialists working on security every day, the resources to detect, prevent, or mitigate cyberattacks are considerable. In fact, while organizations used to worry about whether the cloud was secure, most now understand that the level of investment in people and specialized infrastructure made by vendors like Microsoft makes the cloud more secure than most on-premises datacenters.

Using the cloud can reduce some of the security burden. Microsoft provides physical security for Azure datacenters and helps protect the cloud platform against infrastructure threats such as a DDoS attack. Given that Microsoft has thousands of cybersecurity specialists working on security every day, the resources to detect, prevent, or mitigate cyberattacks are considerable. In fact, while organizations used to worry about whether the cloud was secure, most now understand that the level of investment in people and specialized infrastructure made by vendors like Microsoft makes the cloud more secure than most on-premises datacenters.

Even with this investment in a cloud-native security baseline, it is suggested that any Security Baseline policy extend the default cloud-native policies. The following are examples of extended policies that should be considered, even in a cloud-native environment:

- **Secure VMs.** Security should be every organization's top priority, and doing it effectively requires several things. You must assess your security state, protect against security threats, and then detect and respond rapidly to threats that occur.
- **Protect VM contents.** Setting up regular automated backups is essential to protect against user errors. This isn't enough, though; you must also make sure that your backups are safe from cyberattacks and are available when you need them.
- **Monitor applications.** This pattern encompasses several tasks, including getting insight into the health of your VMs, understanding interactions among them, and establishing ways to monitor the applications these VMs run. All of these tasks are essential in keeping your applications running around the clock.
- **Secure and audit data access.** Organizations should audit all data access and use advanced machine learning capabilities to call out deviations from regular access patterns.
- **Failover practice.** Cloud operations that have low tolerances for failure must be capable of failing over or recovering from a cybersecurity or platform incident. These procedures must not simply be documented, but should be practiced quarterly.

## Next steps

Now that you've reviewed the sample Security Baseline policy for cloud-native solutions, return to the policy review guide to start building on this sample to create your own policies for cloud adoption.

[Build your own policies using the policy review guide](#)

# Microsoft security guidance

11/9/2020 • 5 minutes to read • [Edit Online](#)

## Tools

The [Microsoft Service Trust Portal](#) and Compliance Manager can help meet these needs:

- Overcome compliance management challenges.
- Fulfill responsibilities of meeting regulatory requirements.
- Conduct self-service audits and risk assessments of enterprise cloud service utilization.

These tools are designed to help organizations meet complex compliance obligations and improve data protection capabilities when choosing and using Microsoft cloud services.

The **Microsoft Service Trust Portal** provides in-depth information and tools to help meet your needs for using Microsoft cloud services, including Azure, Microsoft 365, Dynamics 365, and Windows. The portal is a one-stop shop for security, regulatory, compliance, and privacy information related to the Microsoft cloud. It is where we publish the information and resources needed to perform self-service risk assessments of cloud services and tools. The portal was created to help track regulatory compliance activities within Azure, including:

- **Compliance Manager:** Compliance Manager, a workflow-based risk assessment tool in the Microsoft Service Trust Portal, enables you to track, assign, and verify your organization's regulatory compliance activities related to Microsoft cloud services, such as Microsoft 365, Dynamics 365, and Azure. You can find more details in the next section.
- **Trust documents:** Three categories of guides provide abundant resources to assess the Microsoft cloud, learn about Microsoft operations in security, compliance, and privacy, and help you act on improving your data protection capabilities. These guides include:
  - **Audit reports:** Audit reports allow you to stay current on the latest privacy, security, and compliance-related information for Microsoft cloud services. This information includes ISO, SOC, FedRAMP, and other audit reports, bridge letters, and materials related to independent third-party audits of Microsoft cloud services such as Azure, Microsoft 365, Dynamics 365, and others.
  - **Data protection guides:** Data protection guides provide information about how Microsoft cloud services protect your data, and how you can manage cloud data security and compliance for your organization. These guides include detailed white papers about the design and operation of Microsoft cloud services, FAQ documents, reports of end-of-year security assessments, penetration test results, and guidance to help you conduct risk assessment and improve your data protection capabilities.
  - **Azure security and compliance blueprint:** Blueprints provide resources to assist you in building and launching cloud-powered applications that help you comply with stringent regulations and standards. With more certifications than any other cloud provider, you can have confidence deploying your critical workloads to Azure, with blueprints that include:
    - Industry-specific overview and guidance.
    - Customer responsibilities matrix.
    - Reference architectures with threat models.
    - Control implementation matrices.
    - Automation to deploy reference architectures.
    - Privacy resources. Documentation for data protection impact assessments, data subject requests, and data breach notification is provided to incorporate into your own accountability program in support of the General Data Protection Regulation (GDPR).
- **Get started with GDPR:** Microsoft products and services help organizations meet GDPR requirements while

collecting or processing personal data. The Microsoft Service Trust Portal is designed to give you information about the capabilities in Microsoft services that you can use to address specific requirements of the GDPR. The documentation can help your GDPR accountability and your understanding of technical and organizational measures. Documentation for data protection impact assessments, data subject requests, and data breach notification is provided to incorporate into your own accountability program in support of the GDPR.

- **Data subject requests:** The GDPR grants individuals (or data subjects) certain rights in connection with the processing of their personal data. These rights include the right to correct inaccurate data, erase data, or restrict its processing, as well as the right to receive their data and fulfill a request to transmit their data to another controller.
  - **Data breach:** The GDPR mandates notification requirements for data controllers and processors if a breach of personal data occurs. The Microsoft Service Trust Portal provides you with information about how Microsoft works to prevent breaches, how Microsoft detects a breach, and how Microsoft will respond and notify you as a data controller if a breach occurs.
  - **Data protection impact assessment:** Microsoft helps controllers complete GDPR data protection impact assessments (DPIAs). The GDPR provides an inexhaustive list of cases in which DPIAs must be performed, such as automated processing for the purposes of profiling and similar activities; processing on a large scale of special categories of personal data, and systematic monitoring of a publicly accessible area on a large scale.
  - **Other resources:** In addition to tools guidance discussed in the above sections, the Microsoft Service Trust Portal also provides other resources including regional compliance, additional resources for the security and compliance center, and frequently asked questions about the Microsoft Service Trust Portal, Compliance Manager, privacy, and GDPR.
- **Regional compliance:** The Microsoft Service Trust Portal provides numerous compliance documents and guidance for Microsoft online services to meet compliance requirements for different regions including Czech Republic, Poland, and Romania.

## Unique intelligent insights

As the volume and complexity of security signals grow, determining if those signals are credible threats, and then acting, takes far too long. Microsoft offers an unparalleled breadth of security intelligence delivered at cloud scale to help quickly detect and remediate threats. For more information, see the [Azure Security Center overview](#).

## Azure threat intelligence

By using the threat intelligence option available in Security Center, IT administrators can identify security threats against the environment. For example, they can identify whether a particular computer is part of a botnet. Computers can become nodes in a botnet when attackers illicitly install malware that secretly connects the computer to the command and control. Threat intelligence can also identify potential threats coming from underground communication channels, such as the dark web.

To build this threat intelligence, Security Center uses data from multiple sources within Microsoft. Security Center uses this data to identify potential threats against your environment. The threat intelligence pane is composed of three major options:

- Detected threat types
- Threat origin
- Threat intelligence map

## Machine learning in Azure Security Center

Azure Security Center deeply analyzes a wealth of data from a variety of Microsoft and partner solutions to help you achieve greater security. To take advantage of this data, the company use data science and machine learning for threat prevention, detection, and eventually investigation.

Broadly, Azure Machine Learning helps achieve two outcomes:

### **Next-generation detection**

Attackers are increasingly automated and sophisticated. They use data science too. They reverse-engineer protections and build systems that support mutations in behavior. They masquerade their activities as noise, and learn quickly from mistakes. Machine learning helps us respond to these developments.

### **Simplified security baseline**

Making effective security decisions is not easy. It requires security experience and expertise. While some large organizations have such experts on staff, many companies don't. Azure Machine Learning enables customers to benefit from the wisdom of other organizations when making security decisions.

## **Behavioral analytics**

Behavioral analytics is a technique that analyzes and compares data to a collection of known patterns. These patterns are not simple signatures. They're determined through complex machine learning algorithms that are applied to massive data sets. They're also determined through careful analysis of malicious behaviors by expert analysts. Azure Security Center can use behavioral analytics to identify compromised resources based on analysis of virtual machine logs, virtual network device logs, fabric logs, crash dumps, and other sources.

# Security Baseline tools in Azure

11/9/2020 • 2 minutes to read • [Edit Online](#)

The [Security Baseline discipline](#) is one of the [Five Disciplines of Cloud Governance](#). This discipline focuses on ways of establishing policies that protect the network, assets, and most importantly the data that will reside on a cloud provider's solution. Within the Five Disciplines of Cloud Governance, the Security Baseline discipline involves classification of the digital estate and data. It also involves documentation of risks, business tolerance, and mitigation strategies associated with the security of data, assets, and networks. From a technical perspective, this discipline also includes involvement in decisions regarding [encryption](#), [network requirements](#), [hybrid identity strategies](#), and tools to [automate enforcement](#) of security policies across [resource groups](#).

The following list of Azure tools can help mature the policies and processes that support this discipline.

TOOL	AZURE PORTAL AND AZURE RESOURCE MANAGER	AZURE KEY VAULT	AZURE AD	AZURE POLICY	AZURE SECURITY CENTER	AZURE MONITOR
Apply access controls to resources and resource creation	Yes	No	Yes	No	No	No
Secure virtual networks	Yes	No	No	Yes	No	No
Encrypt virtual drives	No	Yes	No	No	No	No
Encrypt PaaS storage and databases	No	Yes	No	No	No	No
Manage hybrid identity services	No	No	Yes	No	No	No
Restrict allowed types of resource	No	No	No	Yes	No	No
Enforce geo-regional restrictions	No	No	No	Yes	No	No
Monitor security health of networks and resources	No	No	No	No	Yes	Yes

TOOL	AZURE PORTAL AND AZURE RESOURCE MANAGER	AZURE KEY VAULT	AZURE AD	AZURE POLICY	AZURE SECURITY CENTER	AZURE MONITOR
Detect malicious activity	No	No	No	No	Yes	Yes
Preemptively detect vulnerabilities	No	No	No	No	Yes	No
Configure backup and disaster recovery	Yes	No	No	No	No	No

For a complete list of Azure security tools and services, see [Security services and technologies available on Azure](#).

Customers commonly use third-party tools to enable Security Baseline discipline activities. For more information, see the article [integrate security solutions in Azure Security Center](#).

In addition to security tools, the [Microsoft Trust Center](#) contains extensive guidance, reports, and related documentation that can help you perform risk assessments as part of your migration planning process.

# Identity Baseline discipline overview

11/9/2020 • 2 minutes to read • [Edit Online](#)

Identity baseline is one of the [Five Disciplines of Cloud Governance](#) within the [Cloud Adoption Framework governance model](#). Identity is increasingly considered the primary security perimeter in the cloud, which is a shift from the traditional focus on network security. Identity services provide the core mechanisms supporting access control and organization within IT environments, and the Identity Baseline discipline complements the [Security Baseline discipline](#) by consistently applying authentication and authorization requirements across cloud adoption efforts.

## NOTE

Identity Baseline discipline does not replace the existing IT teams, processes, and procedures that allow your organization to manage and secure identity services. The primary purpose of this discipline is to identify potential identity-related business risks and provide risk-mitigation guidance to IT staff that are responsible for implementing, maintaining, and operating your identity management infrastructure. As you develop governance policies and processes make sure to involve relevant IT teams in your planning and review processes.

This section of the Cloud Adoption Framework outlines the approach to developing an Identity Baseline discipline as part of your cloud governance strategy. The primary audience for this guidance is your organization's cloud architects and other members of your cloud governance team. The decisions, policies, and processes that emerge from this discipline should involve engagement and discussions with relevant members of the IT teams responsible for implementing and managing your organization's identity management solutions.

If your organization lacks in-house expertise in identity and security, consider engaging external consultants as a part of this discipline. Also consider engaging [Microsoft Consulting Services](#), the [Microsoft FastTrack](#) cloud adoption service, or other external cloud adoption partners to discuss concerns related to this discipline.

## Policy statements

Actionable policy statements and the resulting architecture requirements serve as the foundation of an Identity Baseline discipline. Use [sample policy statements](#) as a starting point for defining your Identity Baseline policies.

### Caution

The sample policies come from common customer experiences. To better align these policies to specific cloud governance needs, execute the following steps to create policy statements that meet your unique business needs.

## Develop governance policy statements

The following steps offer examples and potential options to consider when developing your Identity Baseline discipline. Use each step as a starting point for discussions within your cloud governance team and with affected business, and IT teams across your organization to establish the policies and processes needed to manage identity-related risks.



[Identity Baseline discipline template](#): Download the template for documenting an Identity Baseline discipline.



[Business risks](#): Understand the motives and risks commonly associated with the Identity Baseline discipline.



[Indicators and metrics](#): Indicators to understand whether it is the right time to invest in the Identity Baseline discipline.



[Policy adherence processes](#): Suggested processes for supporting policy compliance in the Identity Baseline discipline.



[Maturity](#): Align cloud management maturity with phases of cloud adoption.



[Toolchain](#): Azure services that can be implemented to support the Identity Baseline discipline.

## Next steps

Get started by evaluating [business risks](#) in a specific environment.

[Understand business risks](#)

# Identity Baseline discipline template

11/9/2020 • 2 minutes to read • [Edit Online](#)

The first step to implementing change is communicating the desired change. The same is true when changing governance practices. The template below serves as a starting point for documenting and communicating policy statements that govern identity services in the cloud.

As your discussions progress, use this template's structure as a model for capturing the business risks, risk tolerances, compliance processes, and tooling needed to define your organization's Identity Baseline policy statements.

## IMPORTANT

This template is a limited sample. Before updating this template to reflect your requirements, you should review the subsequent steps for defining an effective Identity Baseline discipline within your cloud governance strategy.

[Download the Identity Baseline discipline template](#)

## Next steps

Solid governance practices start with an [understanding of business risk](#). Review the article on business risks and begin to document the business risks that align with your current cloud adoption plan.

[Understand business risks](#)

# Motivations and business risks in the Identity Baseline discipline

11/9/2020 • 2 minutes to read • [Edit Online](#)

This article discusses the reasons that customers typically adopt an Identity Baseline discipline within a cloud governance strategy. It also provides a few examples of business risks that drive policy statements.

## Relevance

Traditional on-premises directories are designed to allow businesses to strictly control permissions and policies for users, groups, and roles within their internal networks and datacenters. These directories typically support single-tenant implementations, with services applicable only within the on-premises environment.

Cloud identity services expand an organization's authentication and access control capabilities to the internet. They support multitenancy and can be used to manage users and access policy across cloud applications and deployments. Public cloud platforms have cloud-native identity services supporting management and deployment tasks and are capable of [varying levels of integration](#) with your existing on-premises identity solutions. All of these features can result in cloud identity policy being more complicated than your traditional on-premises solutions require.

The importance of the Identity Baseline discipline to your cloud deployment will depend on the size of your team and need to integrate your cloud-based identity solution with an existing on-premises identity service. Initial test deployments may not require much in the way of user organization or management, but as your cloud estate matures, you will likely need to support more complicated organizational integration and centralized management.

## Business risk

The Identity Baseline discipline attempts to address core business risks related to identity services and access control. Work with your business to identify these risks and monitor each of them for relevance as you plan for and implement your cloud deployments.

Risks will differ between organization, but the following serve as common identity-related risks that you can use as a starting point for discussions within your cloud governance team:

- **Unauthorized access.** Sensitive data and resources that can be accessed by unauthorized users can lead to data leaks or service disruptions, violating your organization's security perimeter and risking business or legal liabilities.
- **Inefficiency due to multiple identity solutions.** Organizations with multiple identity services tenants can require multiple accounts for users. This can lead to inefficiency for users who need to remember multiple sets of credentials and for IT in managing accounts across multiple systems. If user access assignments are not updated across identity solutions as staff, teams, and business goals change, your cloud resources may be vulnerable to unauthorized access or users unable to access required resources.
- **Inability to share resources with external partners.** Difficulty adding external business partners to your existing identity solutions can prevent efficient resource sharing and business communication.
- **On-premises identity dependencies.** Legacy authentication mechanisms or third-party multi-factor authentication might not be available in the cloud, requiring either migrating workloads to be retooled, or additional identity services to be deployed to the cloud. Either requirement could delay or prevent migration, and increase costs.

## Next steps

Use the [Identity Baseline discipline template](#) to document business risks that are likely to be introduced by the current cloud adoption plan.

Once an understanding of realistic business risks is established, the next step is to document the business's tolerance for risk and the indicators and key metrics to monitor that tolerance.

[Understand indicators, metrics, and risk tolerance](#)

# Identity baseline metrics, indicators, and risk tolerance

11/9/2020 • 4 minutes to read • [Edit Online](#)

Learn to quantify business risk tolerance associated with the Identity Baseline discipline. Defining metrics and indicators helps to create a business case for investing in the maturity of this discipline.

## Metrics

Identity management focuses on identifying, authenticating, and authorizing individuals, groups of users, or automated processes, and providing them appropriate access to resources in your cloud deployments. As part of your risk analysis you'll want to gather data related to your identity services to determine how much risk you face, and how important investment in your Identity Baseline discipline is for your planned cloud deployments.

The following are examples of useful metrics that you should gather to help evaluate risk tolerance within the Identity Baseline discipline:

- **Identity systems size.** Total number of users, groups, or other objects managed through your identity systems.
- **Overall size of directory services infrastructure.** Number of directory forests, domains, and tenants used by your organization.
- **Dependency on legacy or on-premises authentication mechanisms.** Number of workloads that depend on legacy or third-party or multi-factor authentication mechanisms.
- **Extent of cloud-deployed directory services.** Number of directory forests, domains, and tenants you've deployed to the cloud.
- **Cloud-deployed Active Directory servers.** Number of Active Directory servers deployed to the cloud.
- **Cloud-deployed organizational units.** Number of Active Directory organizational units (OUs) deployed to the cloud.
- **Extent of federation.** Number of identity management systems federated with your organization's systems.
- **Elevated users.** Number of user accounts with elevated access to resources or management tools.
- **Use of role-based access control.** Number of subscriptions, resource groups, or individual resources not managed through role-based access control (RBAC) via groups.
- **Authentication claims.** Number of successful and failed user authentication attempts.
- **Authorization claims.** Number of successful and failed attempts by users to access resources.
- **Compromised accounts.** Number of user accounts that have been compromised.

## Risk tolerance indicators

Risks related to identity baseline are largely related to the complexity of your organization's identity infrastructure. If all your users and groups are managed using a single directory or cloud-native identity provider using minimal integration with other services, your risk level will likely be small. As your business needs grow, your identity management systems may need to support more complicated scenarios, such as multiple directories to support your internal organization or federation with external identity providers. As these systems become more complex, risk increases.

In the early stages of cloud adoption, work with your IT security team and business stakeholders to identify [business risks](#) related to identity, then determine an acceptable baseline for identity risk tolerance. This section of the Cloud Adoption Framework provides examples, but the detailed risks and baselines for your company or

deployments may be different.

Once you have a baseline, establish minimum benchmarks representing an unacceptable increase in your identified risks. These benchmarks act as triggers for when you need to take action to address these risks. The following are a few examples of how identity related metrics, such as those discussed above, can justify an increased investment in the Identity Baseline discipline.

- **User account number trigger.** A company with more than  $x$  users, groups, or other objects managed in your identity systems could benefit from investment in the Identity Baseline discipline to ensure efficient governance over a large number of accounts.
- **On-premises identity dependency trigger.** A company planning to migrate workloads to the cloud that require legacy authentication capabilities or third-party multi-factor authentication should invest in the Identity Baseline discipline to reduce risks related to refactoring or additional cloud infrastructure deployment.
- **Directory services complexity trigger.** A company maintaining more than  $x$  individual forests, domains, or directory tenants should invest in the Identity Baseline discipline to reduce risks related with account management and the efficiency issues related to multiple user credentials spread across multiple systems.
- **Cloud-hosted directory services trigger.** A company hosting  $x$  Active Directory server virtual machines (VMs) hosted in the cloud, or having  $x$  organizational units (OUs) managed on these cloud-based servers, can benefit from investment in the Identity Baseline discipline to optimize integration with any on-premises or other external identity services.
- **Federation trigger.** A company implementing identity federation with  $x$  external identity management systems can benefit from investing in the Identity Baseline discipline to ensure consistent organizational policy across federation members.
- **Elevated access trigger.** A company with more than  $x\%$  of users with elevated permissions to management tools and resources should consider investing in the Identity Baseline discipline to minimize the risk of inadvertent overprovisioning of access to users.
- **RBAC trigger.** A company with less than  $x\%$  of resources using role-based access control methods should consider investing in the Identity Baseline discipline to identify optimized ways to assign user access to resources.
- **Authentication failure trigger.** A company where authentication failures represent more than  $x\%$  of attempts should invest in the Identity Baseline discipline to ensure that authentication methods are not under external attack, and that users can authenticate properly.
- **Authorization failure trigger.** A company where access attempts are rejected more than  $x\%$  of the time should invest in the Identity Baseline discipline to improve the application and updating of access controls, and identify potentially malicious access attempts.
- **Compromised account trigger.** A company with more than 1 compromised account should invest in the Identity Baseline discipline to improve the strength and security of authentication mechanisms and improve mechanisms to remediate risks related to compromised accounts.

The exact metrics and triggers you use to gauge risk tolerance and the level of investment in the Identity Baseline discipline will be specific to your organization, but the examples above should serve as a useful base for discussion within your cloud governance team.

## Next steps

Use the [Identity Baseline discipline template](#) to document metrics and tolerance indicators that align to the current cloud adoption plan.

Review sample Identity Baseline policies as a starting point to develop your own policies to address specific business risks aligned with your cloud adoption plans.

[Review sample policies](#)

# Identity Baseline sample policy statements

11/9/2020 • 3 minutes to read • [Edit Online](#)

Individual cloud policy statements are guidelines for addressing specific risks identified during your risk assessment process. These statements should provide a concise summary of risks and plans to deal with them. Each statement definition should include these pieces of information:

- **Technical risk:** A summary of the risk this policy will address.
- **Policy statement:** A clear summary explanation of the policy requirements.
- **Design options:** Actionable recommendations, specifications, or other guidance that IT teams and developers can use when implementing the policy.

The following sample policy statements address common identity-related business risks. These statements are examples you can reference when drafting policy statements to address your organization's needs. These examples are not meant to be prescriptive, and there are potentially several policy options for dealing with each identified risk. Work closely with business and IT teams to identify the best policies for your unique set of risks.

## Lack of access controls

**Technical risk:** Insufficient or ad hoc access control settings can introduce risk of unauthorized access to sensitive or mission-critical resources.

**Policy statement:** All assets deployed to the cloud should be controlled using identities and roles approved by current governance policies.

**Potential design options:** [Azure Active Directory Conditional Access](#) is the default access control mechanism in Azure.

## Overprovisioned access

**Technical risk:** Users and groups with control over resources beyond their area of responsibility can result in unauthorized modifications leading to outages or security vulnerabilities.

**Policy statement:** The following policies will be implemented:

- A least-privilege access model will be applied to any resources involved in mission-critical applications or protected data.
- Elevated permissions should be an exception, and any such exceptions must be recorded with the cloud governance team. Exceptions will be audited regularly.

**Potential design options:** Consult the [Azure identity management best practices](#) to implement a role-based access control (RBAC) strategy that restricts access based on the [need to know](#) and [least-privilege security](#) principles.

## Lack of shared management accounts between on-premises and the cloud

**Technical risk:** IT management or administrative staff with accounts on your on-premises Active Directory may not have sufficient access to cloud resources might not be able to efficiently resolve operational or security issues.

**Policy statement:** All groups in the on-premises Active Directory infrastructure that have elevated privileges should be mapped to an approved RBAC role.

**Potential design options:** Implement a hybrid identity solution between your cloud-based Azure Active Directory and your on-premises Active Directory, and add the required on-premises groups to the RBAC roles necessary to do their work.

## Weak authentication mechanisms

**Technical risk:** Identity management systems with insufficiently secure user authentication methods, such as basic user/password combinations, can lead to compromised or hacked passwords, providing a major risk of unauthorized access to secure cloud systems.

**Policy statement:** All accounts are required to sign in to secured resources using a multi-factor authentication method.

**Potential design options:** For Azure Active Directory, implement [Azure Multi-Factor Authentication](#) as part of your user authorization process.

## Isolated identity providers

**Technical risk:** Incompatible identity providers can result in the inability to share resources or services with customers or other business partners.

**Policy statement:** Deployment of any applications that require customer authentication must use an approved identity provider that is compatible with the primary identity provider for internal users.

**Potential design options:** Implement [federation with Azure Active Directory](#) between your internal and customer identity providers or use [Azure Active Directory B2B](#)

## Identity reviews

**Technical risk:** As business changes over time, the addition of new cloud deployments or other security concerns can increase the risks of unauthorized access to secure resources.

**Policy statement:** Cloud governance processes must include quarterly review with identity management teams to identify malicious actors or usage patterns that should be prevented by cloud asset configuration.

**Potential design options:** Establish a quarterly security review meeting that includes both governance team members and IT staff responsible for managing identity services. Review existing security data and metrics to establish gaps in current identity management policy and tooling, and update policy to remediate any new risks.

## Next steps

Use the samples mentioned in this article as a starting point for developing policies to address specific business risks that align with your cloud adoption plans.

To begin developing your own custom Identity Baseline policy statements, download the [Identity Baseline discipline template](#).

To accelerate adoption of this discipline, choose the [actionable governance guide](#) that most closely aligns with your environment. Then modify the design to incorporate your specific corporate policy decisions.

Building on risks and tolerance, establish a process for governing and communicating Identity Baseline policy adherence.

[Establish policy compliance processes](#)

# Identity Baseline policy compliance processes

11/9/2020 • 4 minutes to read • [Edit Online](#)

This article discusses an approach to policy adherence processes that govern the [Identity Baseline discipline](#). Effective governance of identity starts with recurring manual processes that guide identity policy adoption and revisions. This requires regular involvement of the cloud governance team and interested business and IT stakeholders to review and update policy and ensure policy compliance. In addition, many ongoing monitoring and enforcement processes can be automated or supplemented with tooling to reduce the overhead of governance and allow for faster response to policy deviation.

## Planning, review, and reporting processes

Identity management tools offer capabilities and features that greatly assist user management and access control within a cloud deployment. They also require well-considered processes and policies to support your organization's goals. The following is a set of example processes commonly involved in the Identity Baseline discipline. Use these examples as a starting point when planning the processes that will allow you to continue to update identity policy based on business change and feedback from the IT teams tasked with turning governance guidance into action.

**Initial risk assessment and planning:** As part of your initial adoption of the Identity Baseline discipline, identify your core business risks and tolerances related to cloud identity management. Use this information to discuss specific technical risks with members of your IT teams responsible for managing identity services and develop a baseline set of security policies for mitigating these risks to establish your initial governance strategy.

**Deployment planning:** Before any deployment, review the access needs for any workloads and develop an access control strategy that aligns with established corporate identity policy. Document any gaps between needs and current policy to determine whether policy updates are required, and modify policy as needed.

**Deployment testing:** As part of the deployment, the cloud governance team, in cooperation with IT teams responsible for identity services, will be responsible for reviewing the deployment to validate identity policy compliance.

**Annual planning:** On an annual basis, perform a high-level review of identity management strategy. Explore planned changes to the identity services environment and updated cloud adoption strategies to identify potential risk increase or need to modify current identity infrastructure patterns. Also use this time to review the latest identity management best practices and integrate these into your policies and review processes.

**Quarterly planning:** On a quarterly basis perform a general review of identity and access control audit data, and meet with the cloud adoption teams to identify any potential new risks or operational requirements that would require updates to identity policy or changes in access control strategy.

This planning process is also a good time to evaluate the current membership of your cloud governance team for knowledge gaps related to new or changing policy and risks related to identity. Invite relevant IT staff to participate in reviews and planning as either temporary technical advisors or permanent members of your team.

**Education and training:** On a bimonthly basis, offer training sessions to make sure IT staff and developers are up-to-date on the latest identity policy requirements. As part of this process review and update any documentation, guidance, or other training assets to ensure they're in sync with the latest corporate policy statements.

**Monthly audit and reporting reviews:** On a monthly basis, perform an audit on all cloud deployments to assure their continued alignment with identity policy. Use this review to check user access against business change

to ensure users have correct access to cloud resources, and ensure access strategies such as RBAC are being followed consistently. Identify any privileged accounts and document their purpose. This review process produces a report for the cloud strategy team and each cloud adoption team detailing overall adherence to policy. The report is also stored for auditing and legal purposes.

## Processes for ongoing monitoring

A successful Identity Baseline strategy depends on visibility into the current and past state of your identity systems. Without the ability to analyze your cloud deployment's relevant metrics and related data, you cannot identify changes in your risks or detect violations of your risk tolerances. The ongoing governance processes discussed above require quality data to ensure policy can be modified to support the changing needs of your business.

Ensure that your IT teams have implemented automated monitoring systems for your identity services that capture the logs and audit information you need to evaluate risk. Be proactive in monitoring these systems to ensure prompt detection and mitigation of potential policy violation, and ensure any changes to your identity infrastructure are reflected in your monitoring strategy.

## Violation triggers and enforcement actions

Violations of identity policy can result in unauthorized access to sensitive data and lead to serious disruption of mission-critical application and services. When violations are detected, you should take actions to realign with policy as soon as possible. Your IT team can automate most violation triggers using the tools outlined in the [Identity Baseline toolchain](#).

The following triggers and enforcement actions provide examples you can reference when planning how to use monitoring data to resolve policy violations:

- **Suspicious activity detected:** User logins detected from anonymous proxy IP addresses, unfamiliar locations, or successive logins from impossibly distant geographical locations may indicate a potential account breach or malicious access attempt. Login will be blocked until user identity can be verified and password reset.
- **Leaked user credentials:** Accounts that have their username and password leaked to the internet will be disabled until user identity can be verified and password reset.
- **Insufficient access controls detected:** Any protected assets where access restrictions do not meet security requirements will have access blocked until the resource is brought into compliance.

## Next steps

Use the [Identity Baseline discipline template](#) to document the processes and triggers that align to the current cloud adoption plan.

For guidance on executing cloud management policies in alignment with adoption plans, see the article on discipline improvement.

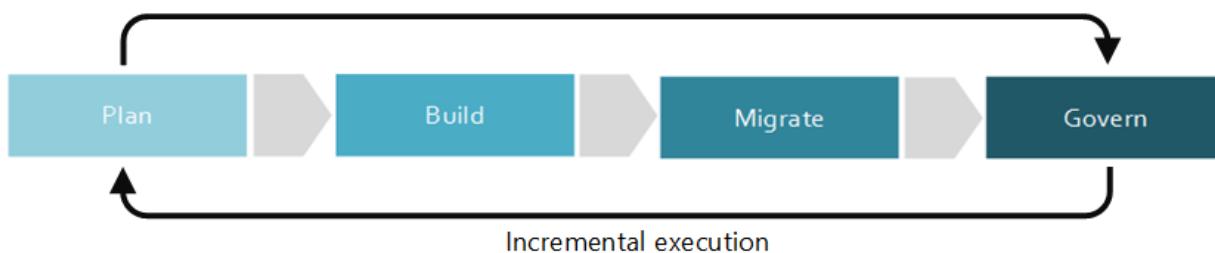
[Identity Baseline discipline improvement](#)

# Identity Baseline discipline improvement

11/9/2020 • 6 minutes to read • [Edit Online](#)

The Identity Baseline discipline focuses on ways of establishing policies that ensure consistency and continuity of user identities regardless of the cloud provider that hosts the application or workload. Within the Five Disciplines of Cloud Governance, the Identity Baseline discipline includes decisions regarding the [hybrid identity strategy](#), evaluation and extension of identity repositories, implementation of single sign-on (same sign-on), auditing and monitoring for unauthorized use or malicious actors. In some cases, it may also involve decisions to modernize, consolidate, or integrate multiple identity providers.

This article outlines some potential tasks your company can engage in to better develop and mature the Identity Baseline discipline. These tasks can be broken down into planning, building, adopting, and operating phases of implementing a cloud solution, which are then iterated on allowing the development of an [incremental approach to cloud governance](#).



*Figure 1: Phases of an incremental approach to cloud governance.*

It's impossible for any one document to account for the requirements of all businesses. As such, this article outlines suggested minimum and potential example activities for each phase of the governance maturation process. The initial objective of these activities is to help you build a [policy MVP](#) and establish a framework for incremental policy improvement. Your cloud governance team will need to decide how much to invest in these activities to improve your Identity Baseline discipline.

**Caution**

Neither the minimum or potential activities outlined in this article are aligned to specific corporate policies or third-party compliance requirements. This guidance is designed to help facilitate the conversations that will lead to alignment of both requirements with a cloud governance model.

## Planning and readiness

This phase of governance maturity bridges the divide between business outcomes and actionable strategies. During this process, the leadership team defines specific metrics, maps those metrics to the digital estate, and begins planning the overall migration effort.

### Minimum suggested activities:

- Evaluate your [Identity Baseline toolchain](#) options and implement a hybrid strategy that is appropriate to your organization.
- Develop a draft architecture guidelines document and distribute to key stakeholders.
- Educate and involve the people and teams affected by the development of architecture guidelines.

### Potential activities:

- Define roles and assignments that will govern identity and access management in the cloud.

- Define your on-premises groups and map to corresponding cloud-based roles.
- Inventory identity providers (including database-driven identities used by custom applications).
- Consolidate and integrate identity providers where duplication exists, to simplify the overall identity solution and reduce risk.
- Evaluate hybrid compatibility of existing identity providers.
- For identity providers that are not hybrid compatible, evaluate consolidation or replacement options.

## Build and predeployment

Several technical and nontechnical prerequisites are required to successfully migrate an environment. This process focuses on the decisions, readiness, and core infrastructure that proceeds a migration.

### Minimum suggested activities:

- Consider a pilot test before implementing your [Identity Baseline toolchain](#), making sure it simplifies the user experience as much as possible.
- Apply feedback from pilot tests into the predeployment. Repeat until results are acceptable.
- Update the architecture guidelines document to include deployment and user adoption plans, and distribute to key stakeholders.
- Consider establishing an early adopter program and rolling out to a limited number of users.
- Continue to educate the people and teams most affected by the architecture guidelines.

### Potential activities:

- Evaluate your logical and physical architecture and determine a [hybrid identity strategy](#).
- Map identity access management policies, such as login ID assignments, and choose the appropriate authentication method for Azure AD.
  - If federated, enable tenant restrictions for administrative accounts.
- Integrate your on-premises and cloud directories.
- Consider using the following access models:
  - [Least-privilege administrative](#) access model.
  - [Privileged Identity Management](#) access model.
- Finalize all preintegration details and review [identity management and access control security best practices](#).
  - Enable single-identity single-sign-on (SSO), also called seamless SSO.
  - Configure multi-factor authentication for administrators.
  - Consolidate or integrate identity providers, where necessary.
  - Implement tooling necessary to centralize management of identities.
  - Enable just-in-time (JIT) access and role change alerting.
  - Conduct a risk analysis of key admin activities for assignment to built-in roles.
  - Consider an updated rollout of stronger authentication for all users.
  - Enable Privileged Identity Management (PIM) for JIT (using time-limited activation) for additional administrative roles.
  - Separate user accounts from global admin accounts, to ensure that administrators do not inadvertently open emails or run programs associated with their global admin accounts).

## Adopt and migrate

Migration is an incremental process that focuses on the movement, testing, and adoption of applications or workloads in an existing digital estate.

### Minimum suggested activities:

- Migrate your [Identity Baseline toolchain](#) from development to production.
- Update the architecture guidelines document and distribute to key stakeholders.
- Develop educational materials and documentation, awareness communications, incentives, and other programs to help drive user adoption.

**Potential activities:**

- Validate that the best practices defined during the build predeployment phases are properly executed.
- Validate and refine your [hybrid identity strategy](#).
- Ensure that each application or workload continues to align with the identity strategy before release.
- Validate that single sign-on (SSO) and seamless SSO is working as expected for your applications.
- Reduce or eliminate the number of alternative identity stores.
- Scrutinize the need for any in-app or in-database identity stores. Identities that fall outside of a proper identity provider (first-party or third-party) can represent risk to the application and the users.
- Enable conditional access for [on-premises federated applications](#).
- Distribute identity across global regions in multiple hubs with synchronization between regions.
- Establish central role-based access control (RBAC) federation.

## Operate and post-implementation

Once the transformation is complete, governance and operations must live on for the natural lifecycle of an application or workload. This phase of governance maturity focuses on the activities that commonly come after the solution is implemented and the transformation cycle begins to stabilize.

**Minimum suggested activities:**

- Customize your [Identity Baseline toolchain](#) based on your organization's changing needs.
- Automate notifications and reports to alert you of potential malicious threats.
- Monitor and report on system usage and user adoption progress.
- Report on post-deployment metrics and distribute to stakeholders.
- Refine the architecture guidelines to guide future adoption processes.
- Communicate and continually educate the affected teams on a periodic basis to ensure ongoing adherence to architecture guidelines.

**Potential activities:**

- Conduct periodic audits of identity policies and adherence practices.
- Ensure sensitive user accounts (such as accounts of corporate executives) are always enabled for multi-factor authentication and anomalous login detection.
- Scan for malicious actors and data breaches regularly, particularly those related to identity fraud, such as potential admin account takeovers.
- Configure a monitoring and reporting tool.
- Consider integrating more closely with security and fraud-prevention systems.
- Regularly review access rights for elevated users or roles.
  - Identify every user who is eligible to activate admin privilege.
- Review onboarding, offboarding, and credential update processes.
- Investigate increasing levels of automation and communication between identity access management (IAM) modules.
- Consider implementing a development security operations (DevSecOps) approach.
- Conduct an impact analysis to gauge results on costs, security, and user adoption.
- Periodically produce an impact report that shows the changes in metrics created by the system and estimate

the business impacts of the [hybrid identity strategy](#).

- Establish integrated monitoring recommended by the [Azure Security Center](#).

## Next steps

Now that you understand the concept of cloud identity governance, examine the [Identity Baseline toolchain](#) to identify Azure tools and features that you'll need when developing the Identity Baseline discipline on the Azure platform.

[Identity Baseline toolchain for Azure](#)

# Identity Baseline tools in Azure

11/9/2020 • 4 minutes to read • [Edit Online](#)

The [Identity Baseline discipline](#) is one of the [Five Disciplines of Cloud Governance](#). This discipline focuses on ways of establishing policies that ensure consistency and continuity of user identities regardless of the cloud provider that hosts the application or workload.

The following tools are included in the discovery guide for hybrid identity.

**Active Directory (on-premises):** Active Directory is the identity provider most frequently used in the enterprise to store and validate user credentials.

**Azure Active Directory:** A software as a service (SaaS) equivalent to Active Directory, capable of federating with an on-premises Active Directory.

**Active Directory (IaaS):** An instance of the Active Directory application running in a virtual machine in Azure.

Identity is the control plane for IT security. So authentication is an organization's access guard to the cloud. Organizations need an identity control plane that strengthens their security and keeps their cloud applications safe from intruders.

## Cloud authentication

Choosing the correct authentication method is the first concern for organizations wanting to move their applications to the cloud.

When you choose this method, Azure AD handles users' sign-in process. Coupled with seamless single sign-on (SSO), users can sign in to cloud applications without having to reenter their credentials. With cloud authentication, you can choose from two options:

**Azure AD password hash synchronization:** The simplest way to enable authentication for on-premises directory objects in Azure AD. This method can also be used with any method as a back-up failover authentication method in case your on-premises server goes down.

**Azure AD Pass-through Authentication:** Provides a persistent password validation for Azure AD authentication services by using a software agent that runs on one or more on-premises servers.

### NOTE

Companies with a security requirement to immediately enforce on-premises user account states, password policies, and sign-in hours should consider the pass-through authentication method.

### Federated authentication:

When you choose this method, Azure AD passes the authentication process to a separate trusted authentication system, such as on-premises Active Directory Federation Services (AD FS) or a trusted third-party federation provider, to validate the user's password.

For a decision tree that helps you choose the best solution for your organization, see [Choose the right authentication method for Azure Active Directory](#).

The following table lists the native tools that can help mature the policies and processes that support this discipline.

CONSIDERATION	PASSWORD HASH SYNCHRONIZATION + SEAMLESS SSO	PASS-THROUGH AUTHENTICATION + SEAMLESS SSO	FEDERATION WITH AD FS
Where does authentication happen?	In the cloud	In the cloud after a secure password verification exchange with the on-premises authentication agent	On-premises
What are the on-premises server requirements beyond the provisioning system: Azure AD Connect?	None	One server for each additional authentication agent	Two or more AD FS servers Two or more WAP servers in the perimeter network
What are the requirements for on-premises internet and networking beyond the provisioning system?	None	<b>Outbound internet access</b> from the servers running authentication agents	<b>Inbound internet access</b> to WAP servers in the perimeter  Inbound network access to AD FS servers from WAP servers in the perimeter  Network load balancing
Is there an SSL certificate requirement?	No	No	Yes
Is there a health monitoring solution?	Not required	Agent status provided by <a href="#">Azure Active Directory admin center</a>	<a href="#">Azure AD Connect Health</a>
Do users get single sign-on to cloud resources from domain-joined devices within the company network?	Yes with <a href="#">Seamless SSO</a>	Yes with <a href="#">Seamless SSO</a>	Yes
What sign-in types are supported?	UserPrincipalName + password  Integrated Windows authentication by using <a href="#">Seamless SSO</a>  <a href="#">Alternate login ID</a>	UserPrincipalName + password  Integrated Windows authentication by using <a href="#">Seamless SSO</a>  <a href="#">Alternate login ID</a>	UserPrincipalName + password  SamAccountName + password  Integrated Windows authentication  <a href="#">Certificate and smart card authentication</a>  <a href="#">Alternate login ID</a>
Is Windows Hello for Business supported?	<a href="#">Key trust model</a>  <a href="#">Certificate trust model with Intune</a>	<a href="#">Key trust model</a>  <a href="#">Certificate trust model with Intune</a>	<a href="#">Key trust model</a>  <a href="#">Certificate trust model</a>

CONSIDERATION	PASSWORD HASH SYNCHRONIZATION + SEAMLESS SSO	PASS-THROUGH AUTHENTICATION + SEAMLESS SSO	FEDERATION WITH AD FS
What are the multi-factor authentication options?	Azure Multi-Factor Authentication  Custom controls with Azure AD Conditional Access*	Azure Multi-Factor Authentication  Custom controls with Azure AD Conditional Access*	Azure Multi-Factor Authentication  Azure Multi-Factor Authentication server  Third-party multi-factor authentication  Custom controls with Azure AD access
What user account states are supported?	Disabled accounts (Up to 30-minute delay)	Disabled accounts  Account locked out  Account expired  Password expired  Sign-in hours	Disabled accounts  Account locked out  Account expired  Password expired  Sign-in hours
What are the Azure AD Conditional Access options?	Azure AD Conditional Access	Azure AD Conditional Access	Azure AD Conditional Access  AD FS claim rules
Is blocking legacy protocols supported?	Yes	Yes	Yes
Can you customize the logo, image, and description on the sign-in pages?	Yes, with Azure AD Premium	Yes, with Azure AD Premium	Yes
What advanced scenarios are supported?	Smart password lockout  Leaked credentials reports	Smart password lockout	Multisite low-latency authentication system  AD FS extranet lockout  Integration with third-party identity systems

#### NOTE

Custom controls in Azure AD Conditional Access does not currently support device registration.

## Next steps

The [Hybrid Identity Digital Transformation Framework white paper](#) outlines combinations and solutions for choosing and integrating each of these components.

The [Azure AD Connect tool](#) helps you to integrate your on-premises directories with Azure AD.

# Resource Consistency discipline overview

11/9/2020 • 2 minutes to read • [Edit Online](#)

Resource consistency is one of the [Five Disciplines of Cloud Governance](#) within the [Cloud Adoption Framework governance model](#). This discipline focuses on ways of establishing policies related to the operational management of an environment, application, or workload. IT operations teams often provide monitoring of applications, workload, and asset performance. They also commonly execute the tasks required to meet scale demands, remediate performance service-level agreement (SLA) violations, and proactively avoid performance SLA violations through automated remediation. Within the Five Disciplines of Cloud Governance, the Resource Consistency discipline ensures resources are consistently configured in such a way that they can be discoverable by IT operations, are included in recovery solutions, and can be onboarded into repeatable operations processes.

## NOTE

Resource Consistency discipline does not replace the existing IT teams, processes, and procedures that allow your organization to effectively manage cloud-based resources. The primary purpose of this discipline is to identify potential business risks and provide risk-mitigation guidance to the IT staff that are responsible for managing your resources in the cloud. As you develop governance policies and processes make sure to involve relevant IT teams in your planning and review processes.

This section of the Cloud Adoption Framework outlines how to develop a Resource Consistency discipline as part of your cloud governance strategy. The primary audience for this guidance is your organization's cloud architects and other members of your cloud governance team. The decisions, policies, and processes that emerge from this discipline should involve engagement and discussions with relevant members of the IT teams responsible for implementing and managing your organization's resource consistency solutions.

If your organization lacks in-house expertise in resource consistency strategies, consider engaging external consultants as a part of this discipline. Also consider engaging [Microsoft Consulting Services](#), the [Microsoft FastTrack](#) cloud adoption service, or other external cloud adoption experts for discussing how best to organize, track, and optimize your cloud-based assets.

## Policy statements

Actionable policy statements and the resulting architecture requirements serve as the foundation of a Resource Consistency discipline. Use [sample policy statements](#). These samples can serve as a starting point for defining your Resource Consistency policies.

### Caution

The sample policies come from common customer experiences. To better align these policies to specific cloud governance needs, execute the following steps to create policy statements that meet your unique business needs.

## Develop governance policy statements

The following steps offer examples and potential options to consider when developing your Resource Consistency discipline. Use each step as a starting point for discussions within your cloud governance team and with affected business, and IT teams across your organization to establish the policies and processes needed to manage Resource Consistency discipline risks.

	<p><a href="#">Resource Consistency discipline template</a>: Download the template for documenting a Resource Consistency discipline.</p>
	<p><a href="#">Business risks</a>: Understand the motives and risks commonly associated with the Resource Consistency discipline.</p>
	<p><a href="#">Indicators and metrics</a>: Indicators to understand whether it is the right time to invest in the Resource Consistency discipline.</p>
	<p><a href="#">Policy adherence processes</a>: Suggested processes for supporting policy compliance in the Resource Consistency discipline.</p>
	<p><a href="#">Maturity</a>: Align cloud management maturity with phases of cloud adoption.</p>
	<p><a href="#">Toolchain</a>: Azure services that can be implemented to support the Resource Consistency discipline.</p>

## Next steps

Get started by evaluating [business risks](#) in a specific environment.

[Understand business risks](#)

# Resource Consistency discipline template

11/9/2020 • 2 minutes to read • [Edit Online](#)

The first step to implementing change is communicating what is desired. The same is true when changing governance practices. The template below serves as a starting point for documenting and communicating policy statements that govern IT operations and management in the cloud.

As your discussions progress, use this template's structure as a model for capturing the business risks, risk tolerances, compliance processes, and tooling needed to define your organization's Resource Consistency policy statements.

## IMPORTANT

This template is a limited sample. Before updating this template to reflect your requirements, you should review the subsequent steps for defining an effective Resource Consistency discipline within your cloud governance strategy.

[Download the Resource Consistency discipline template](#)

## Next steps

Solid governance practices start with an understanding of business risk. Review the article on business risks and begin to document the business risks that align with your current cloud adoption plan.

[Understand business risks](#)

# Motivations and business risks in the Resource Consistency discipline

11/9/2020 • 2 minutes to read • [Edit Online](#)

This article discusses the reasons that customers typically adopt a Resource Consistency discipline within a cloud governance strategy. It also provides a few examples of potential business risks that can drive policy statements.

## Relevance

When it comes to deploying resources and workloads, the cloud offers increased agility and flexibility over most traditional on-premises datacenters. These potential cloud-based advantages also come with potential management drawbacks that can seriously jeopardize the success of your cloud adoption. What assets have you deployed? What teams own what assets? Do you have enough resources supporting a workload? How do you know whether workloads are healthy?

Resource consistency is crucial to ensure that resources are deployed, updated, and configured consistently in a repeatable manner, and that service disruptions are minimized and remedied in as little time as possible.

The Resource Consistency discipline is concerned with identifying and mitigating business risks related to the operational aspects of your cloud deployment. Resource consistency includes monitoring of applications, workloads, and asset performance. It also includes the tasks required to meet scale demands, provide disaster recovery capabilities, mitigate performance service-level agreement (SLA) violations, and proactively avoid those SLA violations through automated remediation.

Initial test deployments may not require much beyond adopting some cursory naming and tagging standards to support your resource consistency needs. As your cloud adoption matures and you deploy more complicated and mission-critical assets, the need to invest in the Resource Consistency discipline increases rapidly.

## Business risk

The Resource Consistency discipline attempts to address core operational business risks. Work with your business and IT teams to identify these risks and monitor each of them for relevance as you plan for and implement your cloud deployments.

Risks will differ between organization, but the following serve as common risks that you can use as a starting point for discussions within your cloud governance team:

- **Unnecessary operational cost.** Obsolete or unused resources, or resources that are overprovisioned during times of low demand, add unnecessary operational costs.
- **Underprovisioned resources.** Resources that experience higher than anticipated demand can result in business disruption as cloud resources are overwhelmed by demand.
- **Management inefficiencies.** Lack of consistent naming and tagging metadata associated with resources can lead to IT staff having difficulty finding resources for management tasks or identifying ownership and accounting information related to assets. This results in management inefficiencies that can increase cost and slow IT responsiveness to service disruption or other operational issues.
- **Business interruption.** Service disruptions that result in violations of your organization's established service-level agreements (SLAs) can result in loss of business or other financial impacts to your company.

## Next steps

Use the [Resource Consistency discipline template](#) to document business risks that are likely to be introduced by the current cloud adoption plan.

Once an understanding of realistic business risks is established, the next step is to document the business's tolerance for risk and the indicators and key metrics to monitor that tolerance.

[Understand indicators, metrics, and risk tolerance](#)

# Risk tolerance metrics and indicators in the Resource Consistency discipline

11/9/2020 • 5 minutes to read • [Edit Online](#)

Learn to quantify business risk tolerance associated with the Resource Consistency discipline. Defining metrics and indicators helps to create a business case for investing in the maturity of this discipline.

## Metrics

Resource consistency focuses on addressing risks related to the operational management of your cloud deployments. As part of your risk analysis you'll want to gather data related to your IT operations to determine how much risk you face, and how important investment in your Resource Consistency discipline is for your planned cloud deployments.

Every organization has different operational scenarios, but the following items represent useful examples of the metrics you should gather when evaluating risk tolerance within the Resource Consistency discipline:

- **Cloud assets.** Total number of cloud-deployed resources.
- **Untagged resources.** Number of resources without required accounting, business impact, or organizational tags.
- **Underused assets.** Number of resources where memory, CPU, or network capabilities are all consistently underutilized.
- **Resource depletion.** Number of resources where memory, CPU, or network capabilities are exhausted by load.
- **Resource age.** Time since resource was last deployed or modified.
- **VMs in critical condition.** Number of deployed VMs where one or more critical issues are detected that must be addressed in order to restore normal functionality.
- **Alerts by severity.** Total number of alerts on a deployed asset, broken down by severity.
- **Unhealthy network links.** Number of resources with network connectivity issues.
- **Unhealthy service endpoints.** Number of issues with external network endpoints.
- **Cloud provider service health incidents.** Number of disruptions or performance incidents caused by the cloud provider.
- **Service-level agreements.** This can include both Microsoft's commitments for uptime and connectivity of Azure services, as well as commitments made by the business to its external and internal customers.
- **Service availability.** Percentage of actual uptime cloud-hosted workloads compared to the expected uptime.
- **Recovery time objective (RTO).** The maximum acceptable time that an application can be unavailable after an incident.
- **Recovery point objective (RPO).** The maximum duration of data loss that is acceptable during a disaster. For example, if you store data in a single database, with no replication to other databases, and perform hourly backups, you could lose up to an hour of data.
- **Mean time to recover (MTTR).** The average time required to restore a component after a failure.
- **Mean time between failures (MTBF).** The duration that a component can reasonably expect to run between outages. This metric can help you calculate how often a service will become unavailable.
- **Backup health.** Number of backups actively being synchronized.
- **Recovery health.** Number of recovery operations successfully performed.

## Risk tolerance indicators

Cloud platforms offer a baseline set of features that allow deployment teams to effectively manage small deployments without extensive additional planning or processes. As a result, small dev/test or experimental first workloads that include a relatively small amount of cloud-based assets represent low level of risk, and will likely not need much in the way of a formal Resource Consistency policy.

As the size of your cloud estate grows the complexity of managing your assets becomes significantly more difficult. With more assets on the cloud, the ability identify ownership of resources and control resource useful becomes critical to minimizing risks. As more mission-critical workloads are deployed to the cloud, service uptime becomes more critical, and tolerance for service disruption potential cost overruns diminishes rapidly.

In the early stages of cloud adoption, work with your IT operations team and business stakeholders to identify [business risks](#) related to resource consistency, then determine an acceptable baseline for risk tolerance. This section of the Cloud Adoption Framework provides examples, but the detailed risks and baselines for your company or deployments may be different.

Once you have a baseline, establish minimum benchmarks representing an unacceptable increase in your identified risks. These benchmarks act as triggers for when you need to take action to remediate these risks. The following are a few examples of how operational metrics, such as those discussed above, can justify an increased investment in the Resource Consistency discipline.

- **Tagging and naming trigger.** A company with more than  $x$  resources lacking required tagging information or not obeying naming standards should consider investing in the Resource Consistency discipline to help refine these standards and ensure consistent application of them to cloud-deployed assets.
- **Overprovisioned resources trigger.** If a company has more than  $x\%$  of assets regularly using small amounts of their available memory, CPU, or network capabilities, investment in the Resource Consistency discipline is suggested to help optimize resources usage for these items.
- **Underprovisioned resources trigger.** If a company has more than  $x\%$  of assets regularly exhausting most of their available memory, CPU, or network capabilities, investment in the Resource Consistency discipline is suggested to help ensure these assets have the resources necessary to prevent service interruptions.
- **Resource age trigger.** A company with more than  $x$  resources that haven't been updated in over  $y$  months could benefit from investment in the Resource Consistency discipline aimed at ensuring active resources are patched and healthy, while retiring obsolete or otherwise unused assets.
- **Service-level agreement trigger.** A company that cannot meet its service-level agreements to its external customers or internal partners should invest in the Deployment Acceleration discipline to reduce system downtime.
- **Recovery time triggers.** If a company exceeds the required thresholds for recovery time following a system failure, it should invest in improving its Deployment Acceleration discipline and systems design to reduce or eliminate failures or the effect of individual component downtime.
- **VM health trigger.** A company that has more than  $x\%$  of VMs experiencing a critical health issue should invest in the Resource Consistency discipline to identify issues and improve VM stability.
- **Network health trigger.** A company that has more than  $x\%$  of network subnets or endpoints experiencing connectivity issues should invest in the Resource Consistency discipline to identify and resolve network issues.
- **Backup coverage trigger.** A company with  $x\%$  of mission-critical assets without up-to-date backups in place would benefit from an increased investment in the Resource Consistency discipline to ensure a consistent backup strategy.
- **Backup health trigger.** A company experiencing more than  $x\%$  failure of restore operations should invest in the Resource Consistency discipline to identify problems with backup and ensure important resources are protected.

The exact metrics and triggers you use to gauge risk tolerance and the level of investment in the Resource Consistency discipline will be specific to your organization, but the examples above should serve as a useful base

for discussion within your cloud governance team.

## Next steps

Use the [Resource Consistency discipline template](#) to document metrics and tolerance indicators that align to the current cloud adoption plan.

Review sample Resource Consistency policies as a starting point to develop your own policies to address specific business risks aligned with your cloud adoption plans.

[Review sample policies](#)

# Resource Consistency sample policy statements

11/9/2020 • 4 minutes to read • [Edit Online](#)

Individual cloud policy statements are guidelines for addressing specific risks identified during your risk assessment process. These statements should provide a concise summary of risks and plans to deal with them. Each statement definition should include these pieces of information:

- **Technical risk:** A summary of the risk this policy will address.
- **Policy statement:** A clear summary explanation of the policy requirements.
- **Design options:** Actionable recommendations, specifications, or other guidance that IT teams and developers can use when implementing the policy.

The following sample policy statements address common business risks related to resource consistency. These statements are examples you can reference when drafting policy statements to address your organization's needs. These examples are not meant to be prescriptive, and there are potentially several policy options for dealing with each identified risk. Work closely with business and IT teams to identify the best policies for your unique set of risks.

## Tagging

**Technical risk:** Without proper metadata tagging associated with deployed resources, IT operations cannot prioritize support or optimization of resources based on required SLA, importance to business operations, or operational cost. This can result in mis-allocation of IT resources and potential delays in incident resolution.

**Policy statement:** The following policies will be implemented:

- Deployed assets should be tagged with the following values:
  - Cost
  - Criticality
  - SLA
  - Environment
- Governance tooling must validate tagging related to cost, criticality, SLA, application, and environment. All values must align to predefined values managed by the governance team.

**Potential design options:** In Azure, [standard name-value metadata tags](#) are supported on most resource types. [Azure Policy](#) is used to enforce specific tags as part of resource creation.

## Ungoverned subscriptions

**Technical risk:** Arbitrary creation of subscriptions and management groups can lead to isolated sections of your cloud estate that are not properly subject to your governance policies.

**Policy statement:** Creation of new subscriptions or management groups for any mission-critical applications or protected data will require a review from the cloud governance team. Approved changes will be integrated into a proper blueprint assignment.

**Potential design options:** Lock down administrative access to your organizations [Azure management groups](#) to only approved governance team members who will control the subscription creation and access control process.

## Manage updates to virtual machines

**Technical risk:** Virtual machines (VMs) that are not up-to-date with the latest updates and software patches are vulnerable to security or performance issues, which can result in service disruptions.

**Policy statement:** Governance tooling must enforce that automatic updates are enabled on all deployed VMs. Violations must be reviewed with operational management teams and remediated in accordance with operations policies. Assets that are not automatically updated must be included in processes owned by IT operations.

**Potential design options:** For Azure hosted VMs, you can provide consistent update management using the [update management solution in Azure Automation](#).

## Deployment compliance

**Technical risk:** Deployment scripts and automation tooling that is not fully vetted by the cloud governance team can result in resource deployments that violate policy.

**Policy statement:** The following policies will be implemented:

- Deployment tooling must be approved by the cloud governance team to ensure ongoing governance of deployed assets.
- Deployment scripts must be maintained in central repository accessible by the cloud governance team for periodic review and auditing.

**Potential design options:** Consistent use of [Azure Blueprints](#) to manage automated deployments allows consistent deployments of Azure resources that adhere to your organization's governance standards and policies.

## Monitoring

**Technical risk:** Improperly implemented or inconsistently instrumented monitoring can prevent the detection of workload health issues or other policy compliance violations.

**Policy statement:** The following policies will be implemented:

- Governance tooling must validate that all assets are included in monitoring for resource depletion, security, compliance, and optimization.
- Governance tooling must validate that the appropriate level of logging data is being collected for all applications and data.

**Potential design options:** [Azure Monitor](#) is the default monitoring service in Azure, and consistent monitoring can be enforced via [Azure Blueprints](#) when deploying resources.

## Disaster recovery

**Technical risk:** Resource failure, deletions, or corruption can result in disruption of mission-critical applications or services and the loss of sensitive data.

**Policy statement:** All mission-critical applications and protected data must have backup and recovery solutions implemented to minimize business impact of outages or system failures.

**Potential design options:** The [Azure Site Recovery](#) service provides backup, recovery, and replication capabilities that minimize outage duration in business continuity and disaster recovery (BCDR) scenarios.

## Next steps

Use the samples mentioned in this article as a starting point to develop policies that address specific business risks that align with your cloud adoption plans.

To begin developing your own custom Resource Consistency policy statements, download the [Resource](#)

## [Consistency discipline template.](#)

To accelerate adoption of this discipline, choose the [actionable governance guide](#) that most closely aligns with your environment. Then modify the design to incorporate your specific corporate policy decisions.

Building on risks and tolerance, establish a process for governing and communicating Resource Consistency policy adherence.

### [Establish policy compliance processes](#)

# Resource Consistency policy compliance processes

11/9/2020 • 5 minutes to read • [Edit Online](#)

This article discusses an approach to policy adherence processes that govern [resource consistency](#). Effective cloud resource consistency governance starts with recurring manual processes designed to identify operational inefficiencies, improve management of deployed resources, and ensure mission-critical workloads have minimal disruptions. These manual processes are supplemented with monitoring, automation, and tooling to help reduce the overhead of governance and allow for faster response to policy deviation.

## Planning, review, and reporting processes

Cloud platforms provide an array of management tools and features that you can use to organize, provision, scale, and minimize downtime. Using these tools to effectively structure and operate your cloud deployments in ways that remediate potential risks requires well-considered processes and policies in addition to close cooperation with IT operations teams and business stakeholders.

The following is a set of example processes commonly involved in the Resource Consistency discipline. Use these examples as a starting point when planning the processes that will allow you to continue to update Resource Consistency policy based on business change and feedback from the development and IT teams tasked with turning guidance into action.

**Initial risk assessment and planning:** As part of your initial adoption of the Resource Consistency discipline, identify your core business risks and tolerances related to operations and IT management. Use this information to discuss specific technical risks with members of your IT teams and workload owners to develop a baseline set of Resource Consistency policies designed to remediate these risks, establishing your initial governance strategy.

**Deployment planning:** Before deploying any asset, perform a review to identify any new operational risks. Establish resource requirements and expected demand patterns, and identify scalability needs and potential usage optimization opportunities. Also ensure backup and recovery plans are in place.

**Deployment testing:** As part of deployment, the cloud governance team, in cooperation with your cloud operations teams, will be responsible for reviewing the deployment to validate Resource Consistency policy compliance.

**Annual planning:** On an annual basis, perform a high-level review of Resource Consistency strategy. Explore future corporate expansion plans or priorities and update cloud adoption strategies to identify potential risk increase or other emerging resource consistency needs. Also use this time to review the latest best practices for cloud resource consistency and integrate these into your policies and review processes.

**Quarterly review and planning:** On a quarterly basis perform a review of operational data and incident reports to identify any changes required in Resource Consistency policy. As part of this process, review changes in resource usage and performance to identify assets that require increases or decreases in resource allocation, and identify any workloads or assets that are candidates for retirement.

This planning process is also a good time to evaluate the current membership of your cloud governance team for knowledge gaps related to new or changing policy and risks associated with the Resource Consistency discipline. Invite relevant IT staff to participate in reviews and planning as either temporary technical advisors or permanent members of your team.

**Education and training:** On a bimonthly basis, offer training sessions to make sure IT staff and developers are up-to-date on the latest Resource Consistency policy requirements and guidance. As part of this process review and update any documentation or other training assets to ensure they're in sync with the latest corporate policy

statements.

**Monthly audit and reporting reviews:** On a monthly basis, perform an audit on all cloud deployments to assure their continued alignment with Resource Consistency policy. Review related activities with IT staff and identify any compliance issues not already handled as part of the ongoing monitoring and enforcement process. The result of this review is a report for the cloud strategy team and each cloud adoption team to communicate overall performance and adherence to policy. The report is also stored for auditing and legal purposes.

## Processes for ongoing monitoring

A successful Resource Consistency strategy depends on visibility into the current and past state of your cloud infrastructure. Without the ability to analyze the relevant metrics and data of your cloud environment's health and activity, you cannot identify changes in your risks or detect violations of your risk tolerances. The ongoing governance processes discussed above require quality data to ensure policy can be modified to optimize your cloud resource usage and improve overall performance of cloud-hosted workloads.

Ensure that your IT teams have implemented automated monitoring systems for your cloud infrastructure that capture the relevant logs data you need to evaluate risks. Be proactive in monitoring these systems to ensure prompt detection and mitigation of potential policy violation, and ensure your monitoring strategy is in line with your operational needs.

## Violation triggers and enforcement actions

Because Resource Consistency policy compliance can lead to critical service disruption or significant cost overruns risks, the cloud governance team should have visibility into noncompliance incidents. Ensure IT staff have clear escalation paths for reporting these issues to the governance team members best suited to identify and verify that policy issues are mitigated when detected.

When violations are detected, you should take actions to realign with policy as soon as possible. Your IT team can automate most violation triggers using the tools outlined in the [Resource Consistency toolchain for Azure](#).

The following triggers and enforcement actions provide examples you can reference when planning how to use monitoring data to resolve policy violations:

- **Overprovisioned resource detected.** Resources detected using less than 60% of CPU or memory capacity should automatically scale down or deprovisioning resources to reduce costs.
- **Underprovisioned resource detected.** Resources detected using more than 80% of CPU or memory capacity should automatically scale up or provisioning additional resources to provide additional capacity.
- **Untagged resource creation.** Any request to create a resource without required meta tags will be rejected automatically.
- **Critical resource outage detected.** IT staff are notified on all detected outages of mission-critical outages. If outage is not immediately resolvable, staff will escalate the issue and notify workload owners and the cloud governance team. The cloud governance team will track the issue until resolution and update guidance if policy revision is necessary to prevent future incidents.
- **Configuration drift.** Resources detected that do not conform to established baselines should trigger alerts and be automatically remediated using configuration management tools like Azure Automation, Chef, Puppet, or Ansible.

## Next steps

Use the [Resource Consistency discipline template](#) to document the processes and triggers that align to the current cloud adoption plan.

For guidance on executing cloud management policies in alignment with adoption plans, see the article on discipline improvement.

Resource Consistency discipline improvement

# Resource Consistency discipline improvement

11/9/2020 • 6 minutes to read • [Edit Online](#)

The Resource Consistency discipline focuses on ways of establishing policies related to the operational management of an environment, application, or workload. Within the Five Disciplines of Cloud Governance, the Resource Consistency discipline includes the monitoring of application, workload, and asset performance. It also includes the tasks required to meet scale demands, remediate performance service-level agreement (SLA) violations, and proactively avoid SLA violations through automated remediation.

This article outlines some potential tasks your company can engage in to better develop and mature the Resource Consistency discipline. These tasks can be broken down into planning, building, adopting, and operating phases of implementing a cloud solution, which are then iterated on allowing the development of an [incremental approach to cloud governance](#).

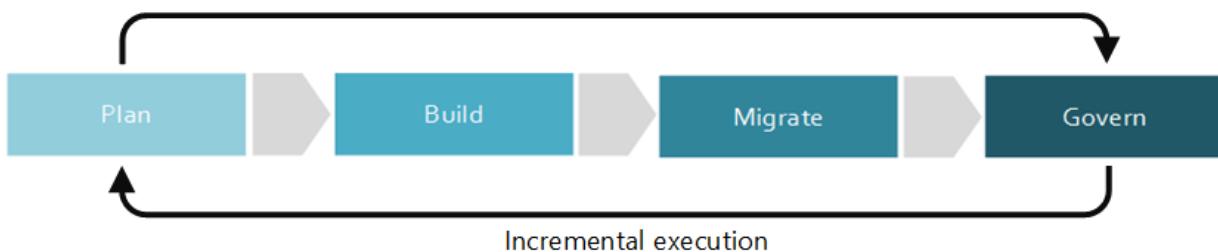


Figure 1: Phases of an incremental approach to cloud governance.

It's impossible for any one document to account for the requirements of all businesses. As such, this article outlines suggested minimum and potential example activities for each phase of the governance maturation process. The initial objective of these activities is to help you build a [policy MVP](#) and establish a framework for incremental policy improvement. Your cloud governance team will need to decide how much to invest in these activities to improve your Resource Consistency discipline.

**Caution**

Neither the minimum or potential activities outlined in this article are aligned to specific corporate policies or third-party compliance requirements. This guidance is designed to help facilitate the conversations that will lead to alignment of both requirements with a cloud governance model.

## Planning and readiness

This phase of governance maturity bridges the divide between business outcomes and actionable strategies. During this process, the leadership team defines specific metrics, maps those metrics to the digital estate, and begins planning the overall migration effort.

### Minimum suggested activities:

- Evaluate your [Resource Consistency toolchain](#) options.
- Understand the licensing requirements for your cloud strategy.
- Develop a draft architecture guidelines document and distribute to key stakeholders.
- Become familiar with the Resource Manager you use to deploy, manage, and monitor all the resources for your solution as a group.
- Educate and involve the people and teams affected by the development of architecture guidelines.
- Add prioritized resource deployment tasks to your migration backlog.

#### Potential activities:

- Work with the business stakeholders and your cloud strategy team to understand the desired cloud accounting approach and cost accounting practices within your business units and organization as a whole.
- Define your [monitoring and policy enforcement](#) requirements.
- Examine the business value and cost of outage to define remediation policy and SLA requirements.
- Determine whether you'll deploy a [simple workload](#) or [multiple team](#) governance strategy for your resources.
- Determine scalability requirements for your planned workloads.

## Build and predeployment

Several technical and nontechnical prerequisites are required to successfully migrate an environment. This process focuses on the decisions, readiness, and core infrastructure that precede a migration.

#### Minimum suggested activities:

- Implement your [Resource Consistency toolchain](#) by rolling out in a predeployment phase.
- Update the architecture guidelines document and distribute to key stakeholders.
- Implement resource deployment tasks on your prioritized migration backlog.
- Develop educational materials and documentation, awareness communications, incentives, and other programs to help drive user adoption.

#### Potential activities:

- Decide on a [subscription design strategy](#), choosing the subscription patterns that best fit your organization and workload needs.
- Use a [resource consistency](#) strategy to enforce architecture guidelines over time.
- Implement [resource naming, and tagging standards](#) for your resources to match your organizational and accounting requirements.
- To create proactive point-in-time governance, use deployment templates and automation to enforce common configurations and a consistent grouping structure when deploying resources and resource groups.
- Establish a least-privilege permissions model, where users have no permissions by default.
- Determine who in your organization owns each workload and account, and who will need to access to maintain or modify these resources. Define cloud roles and responsibilities that match these needs and use these roles as the basis for access control.
- Define dependencies between resources.
- Implement automated resource scaling to match requirements defined in the Plan phase.
- Conduct access performance to measure the quality of services received.
- Consider deploying [Azure Policy](#) to manage SLA enforcement using configuration settings and resource creation rules.

## Adopt and migrate

Migration is an incremental process that focuses on the movement, testing, and adoption of applications or workloads in an existing digital estate.

#### Minimum suggested activities:

- Migrate your [Resource Consistency toolchain](#) from predeployment to production.
- Update the architecture guidelines document and distribute to key stakeholders.
- Develop educational materials and documentation, awareness communications, incentives, and other programs to help drive user adoption.
- Migrate any existing automated remediation scripts or tools to support defined SLA requirements.

#### Potential activities:

- Complete and test monitoring and reporting data with your chosen on-premises, cloud gateway, or hybrid solution.
- Determine whether changes need to be made to SLA or management policy for resources.
- Improve operations tasks by implementing query capabilities to efficiently find resource across your cloud estate.
- Align resources to changing business needs and governance requirements.
- Ensure that your virtual machines, virtual networks, and storage accounts reflect actual resource access needs during each release, and adjust as necessary.
- Verify automated scaling of resources meets access requirements.
- Review user access to resources, resource groups, and Azure subscriptions, and adjust access controls as necessary.
- Monitor changes in resource access plans and validate with stakeholders if additional sign-offs are needed.
- Update changes to the architecture guidelines document to reflect actual costs.
- Determine whether your organization requires clearer financial alignment to P&Ls for business units.
- For global organizations, implement your SLA compliance or sovereignty requirements.
- For cloud aggregation, deploy a gateway solution to a cloud provider.
- For tools that don't allow for hybrid or gateway options, tightly couple monitoring with an operational monitoring tool that spans all datacenters and clouds.

## Operate and post-implementation

Once the transformation is complete, governance and operations must live on for the natural lifecycle of an application or workload. This phase of governance maturity focuses on the activities that commonly come after the solution is implemented and the transformation cycle begins to stabilize.

#### Minimum suggested activities:

- Customize your [Resource Consistency toolchain](#) based on your organization's changing needs.
- Consider automating any notifications and reports to reflect actual resource usage.
- Refine architecture guidelines to guide future adoption processes.
- Educate affected teams periodically to ensure ongoing adherence to the architecture guidelines.

#### Potential activities:

- Adjust plans quarterly to reflect changes to actual resources.
- Automatically apply and enforce governance requirements during future deployments.
- Evaluate underused resources and determine whether they're worth continuing.
- Detect misalignments and anomalies between planned and actual resource usage.
- Assist the cloud adoption teams and the cloud strategy team in understanding and resolving these anomalies.
- Determine whether changes need to be made to your Resource Consistency discipline for billing and SLAs.
- Evaluate logging and monitoring tools to determine whether your on-premises, cloud gateway, or hybrid solution needs adjusting.
- For business units and geographically distributed groups, determine whether your organization should consider using additional cloud management features such as [Azure management groups](#) to better apply centralized policy and meet SLA requirements.

## Next steps

Now that you understand the concept of cloud resource governance, move on to learn more about [how resource access is managed](#) in Azure in preparation for learning how to design a governance model for a [simple workload](#).

or for [multiple teams](#).

[Learn about resource access management in Azure](#) [Learn about service-level agreements for Azure](#) [Learn about logging, reporting, and monitoring](#)

# Resource Consistency tools in Azure

11/9/2020 • 2 minutes to read • [Edit Online](#)

**Resource consistency** is one of the [Five Disciplines of Cloud Governance](#). This discipline focuses on ways of establishing policies related to the operational management of an environment, application, or workload. Within the Five Disciplines of Cloud Governance, the Resource Consistency discipline involves monitoring of application, workload, and asset performance. It also involves the tasks required to meet scale demands, remediate performance SLA violations, and proactively avoid performance SLA violations through automated remediation.

The following is a list of Azure tools that can help mature the policies and processes that support this discipline.

TOOL	AZURE PORTAL	AZURE RESOURCE MANAGER	AZURE BLUEPRINTS	AZURE AUTOMATION	AZURE AD	AZURE BACKUP	AZURE SITE RECOVERY
Deploy resources	Yes	Yes	Yes	Yes	No	No	No
Manage resources	Yes	Yes	Yes	Yes	No	No	No
Deploy resources using templates	No	Yes	No	Yes	No	No	No
Orchestrated environment deployment	No	No	Yes	No	No	No	No
Define resource groups	Yes	Yes	Yes	No	No	No	No
Manage workload and account owners	Yes	Yes	Yes	No	No	No	No
Manage conditional access to resources	Yes	Yes	Yes	No	No	No	No
Configure RBAC users	Yes	No	No	No	Yes	No	No

Tool	Azure Portal	Azure Resource Manager	Azure Blueprints	Azure Automation	Azure AD	Azure Backup	Azure Site Recovery
Assign roles and permissions to resources	Yes	Yes	Yes	No	Yes	No	No
Define dependencies between resources	No	Yes	Yes	No	No	No	No
Apply access control	Yes	Yes	Yes	No	Yes	No	No
Assess availability and scalability	No	No	No	Yes	No	No	No
Apply tags to resources	Yes	Yes	Yes	No	No	No	No
Assign Azure Policy rules	Yes	Yes	Yes	No	No	No	No
Apply automated remediation	No	No	No	Yes	No	No	No
Manage billing	Yes	No	No	No	No	No	No
Plan resources for disaster recovery	Yes	Yes	Yes	No	No	Yes	Yes
Recover data during an outage or SLA violation	No	No	No	No	No	Yes	Yes
Recover applications and data during an outage or SLA violation	No	No	No	No	No	Yes	Yes

Along with these Resource Consistency tools and features, you will need to monitor your deployed resources for

performance and health issues. [Azure Monitor](#) is the default monitoring and reporting solution in Azure. Azure Monitor provides features for monitoring your cloud resources. This list shows which feature addresses common monitoring requirements.

TOOL	AZURE PORTAL	APPLICATION INSIGHTS	LOG ANALYTICS	AZURE MONITOR REST API
Log virtual machine telemetry data	No	No	Yes	No
Log virtual networking telemetry data	No	No	Yes	No
Log PaaS services telemetry data	No	No	Yes	No
Log application telemetry data	No	Yes	No	No
Configure reports and alerts	Yes	No	No	Yes
Schedule regular reports or custom analysis	No	No	No	No
Visualize and analyze log and performance data	Yes	No	No	No
Integrate with on-premises or third-party monitoring solution	No	No	No	Yes

When planning your deployment, you will need to consider where logging data is stored and how you integrate cloud-based [reporting and monitoring services](#) with your existing processes and tools.

#### NOTE

Organizations also use third-party DevOps tools to monitor workloads and resources. For more information, see [DevOps tool integrations](#).

## Next steps

Learn to create, assign, and manage [policy definitions](#) in Azure.

# Resource access management in Azure

11/9/2020 • 4 minutes to read • [Edit Online](#)

The [Govern methodology](#) outlines the Five Disciplines of Cloud Governance, which includes resource management. [What is resource access governance](#) furthers explains how resource access management fits into the resource management discipline. Before you move on to learn how to design a governance model, it's important to understand the resource access management controls in Azure. The configuration of these resource access management controls forms the basis of your governance model.

Begin by taking a closer look at how resources are deployed in Azure.

## What is an Azure resource?

In Azure, the term *resource* refers to an entity managed by Azure. For example, virtual machines, virtual networks, and storage accounts are all referred to as Azure resources.

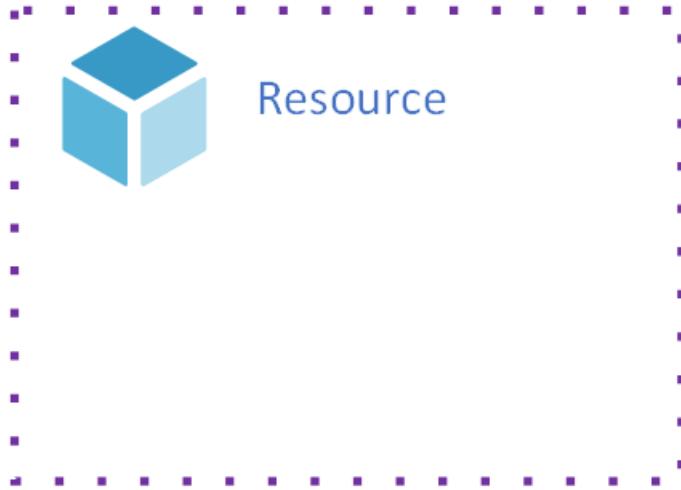
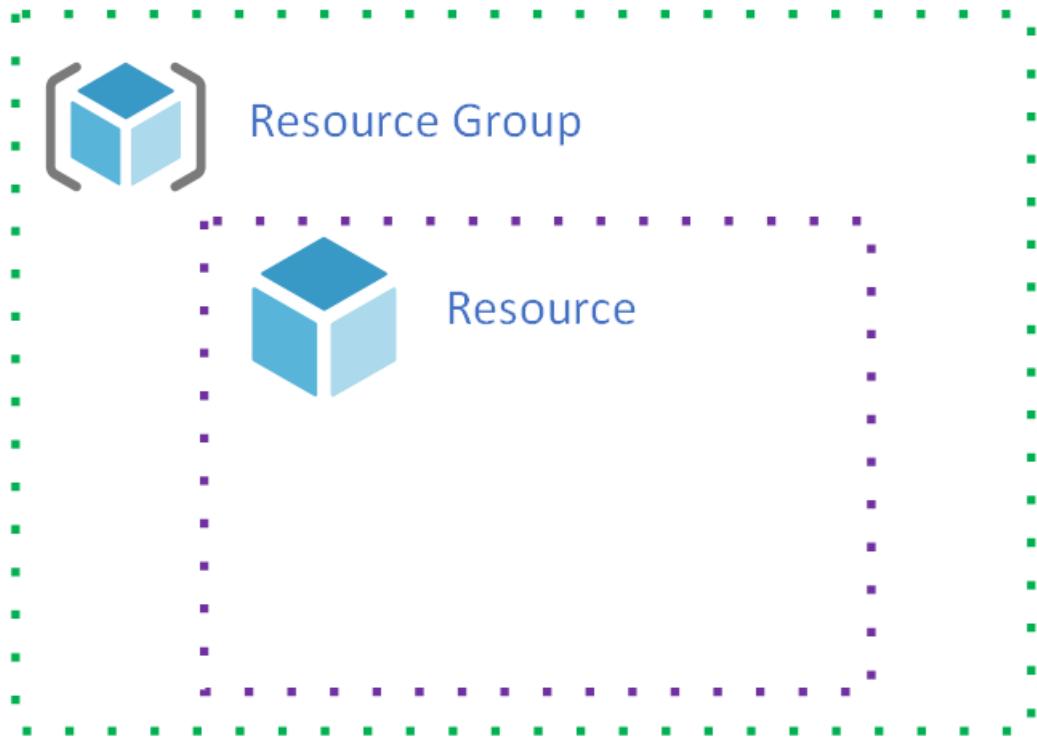


Figure 1: A resource.

## What is an Azure resource group?

Each resource in Azure must belong to a [resource group](#). A resource group is simply a logical construct that groups multiple resources together so they can be managed as a single entity **based on lifecycle and security**. For example, resources that share a similar lifecycle, such as the resources for an [n-tier application](#) may be created or deleted as a group. In other words, everything that is born together, gets managed together, and deprecates together, goes together in a resource group.



Figure

2: A resource group contains a resource.

Resource groups and the resources they contain are associated with an Azure subscription.

## What is an Azure subscription?

An Azure *subscription* is similar to a resource group in that it's a logical construct that groups together resource groups and their resources. An Azure subscription is also associated with the controls used by Azure Resource Manager. Take a closer look at Azure Resource Manager to learn about the relationship between it and an Azure subscription.

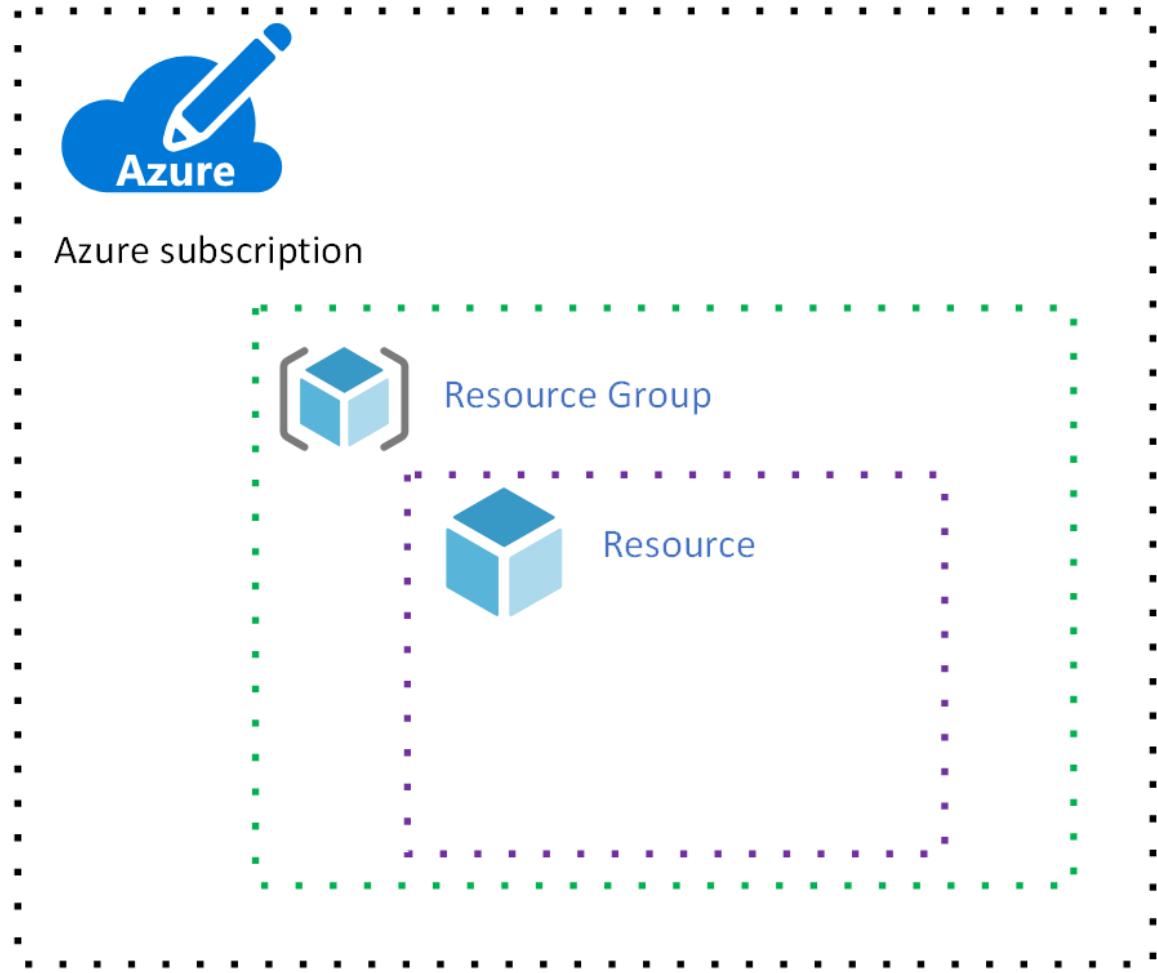


Figure 3: An Azure subscription.

## What is Azure Resource Manager?

In [How does Azure work?](#) you learned that Azure includes a front end with many services that orchestrate all the functions of Azure. One of these services is [Azure Resource Manager](#), and this service hosts the RESTful API used by clients to manage resources.

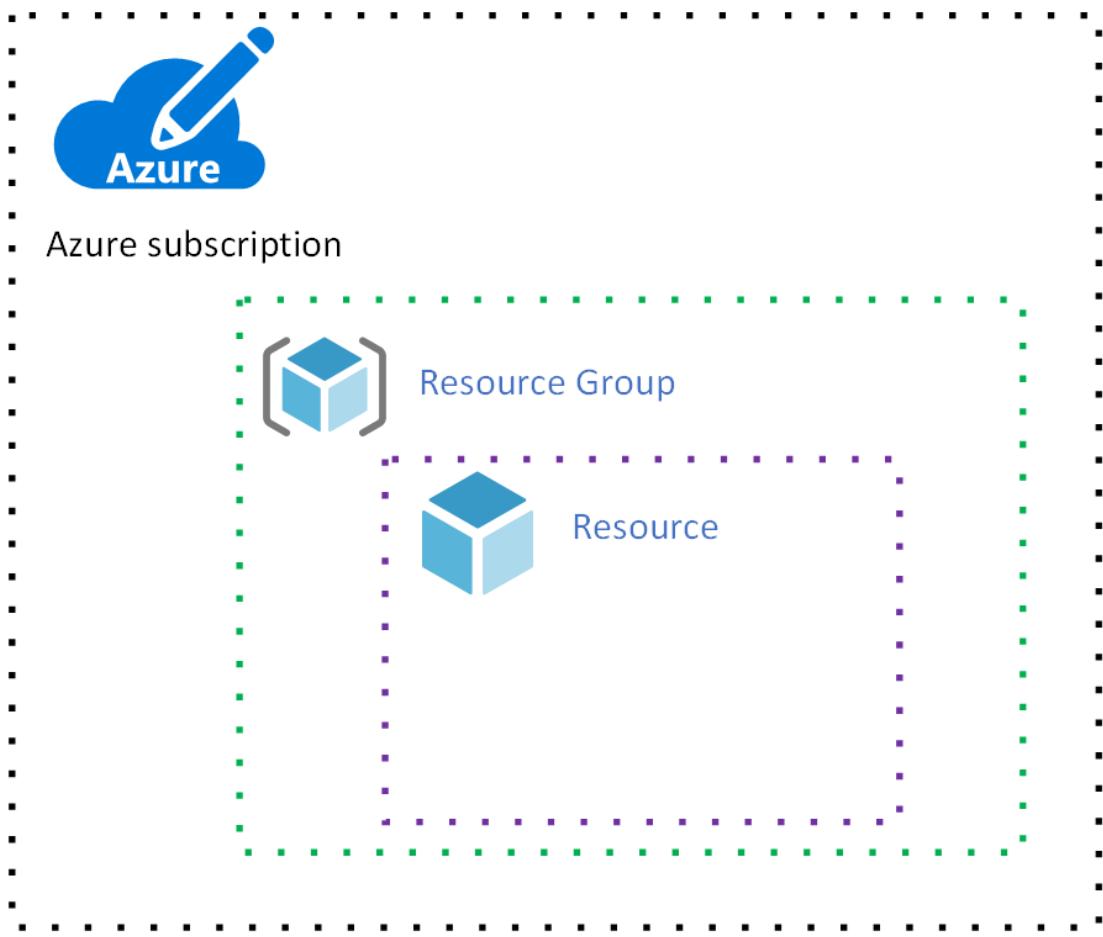
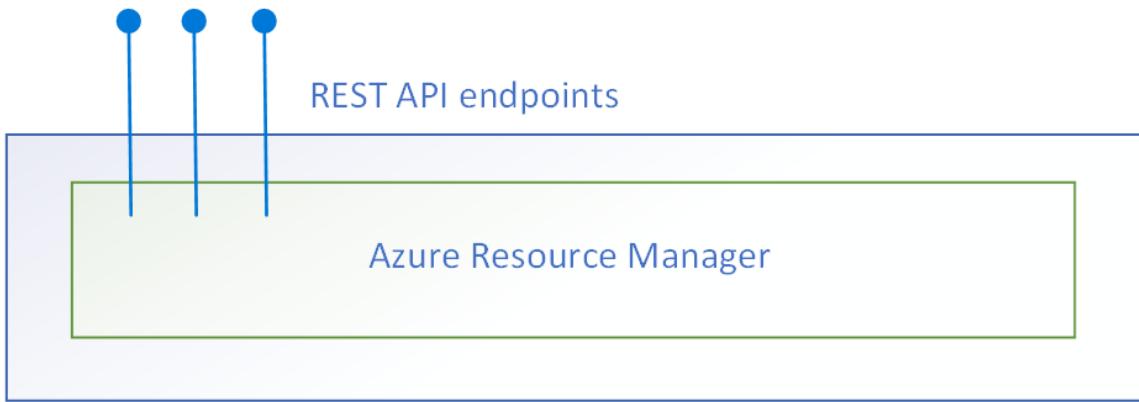


Figure 4: Azure Resource Manager.

The following figure shows three clients: [PowerShell](#), the [Azure portal](#), and the [Azure CLI](#):

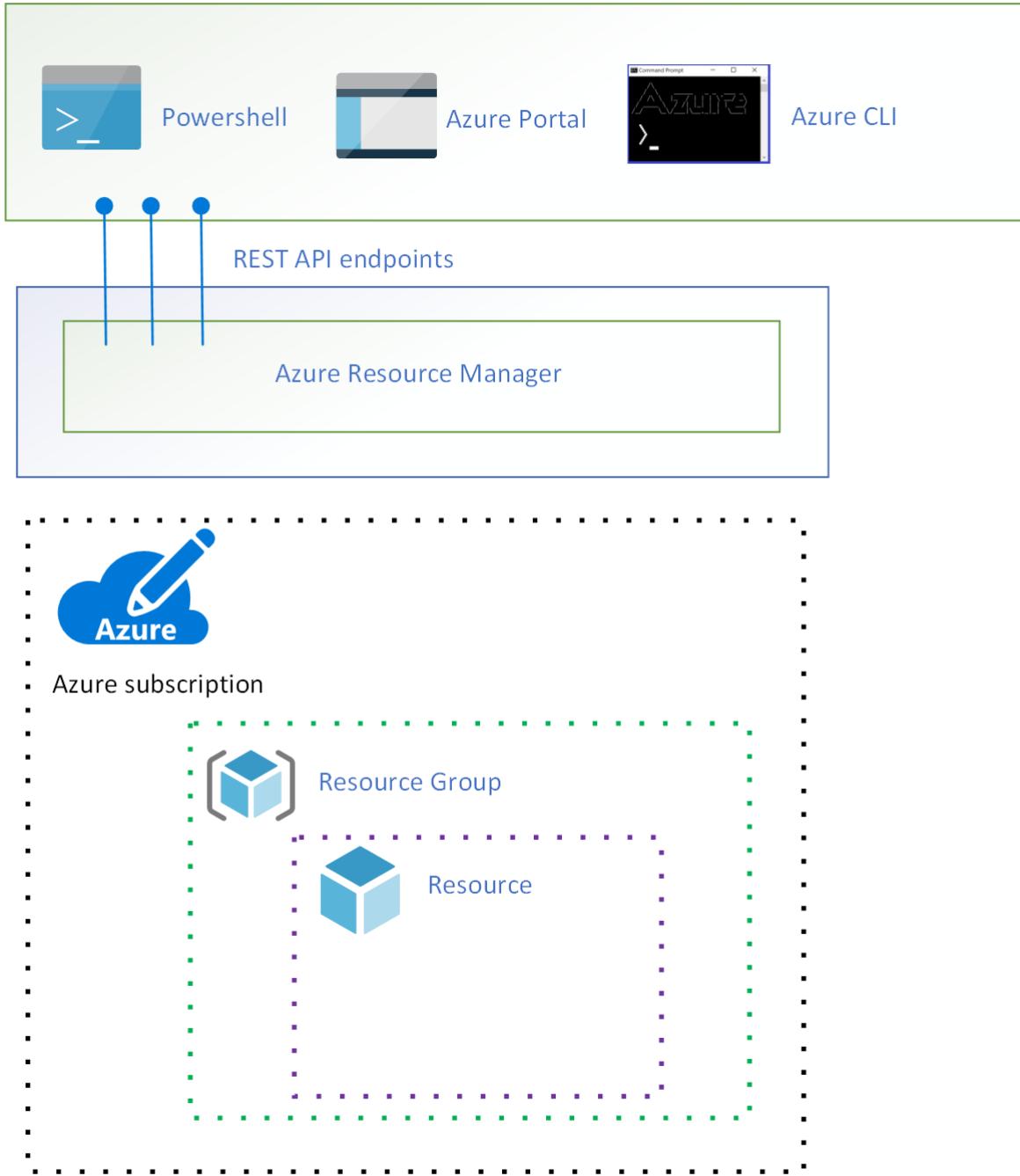


Figure 5: Azure clients connect to the Resource Manager REST API.

While these clients connect to Resource Manager using the REST API, Resource Manager does not include functionality to manage resources directly. Rather, most resource types in Azure have their own [resource provider](#).

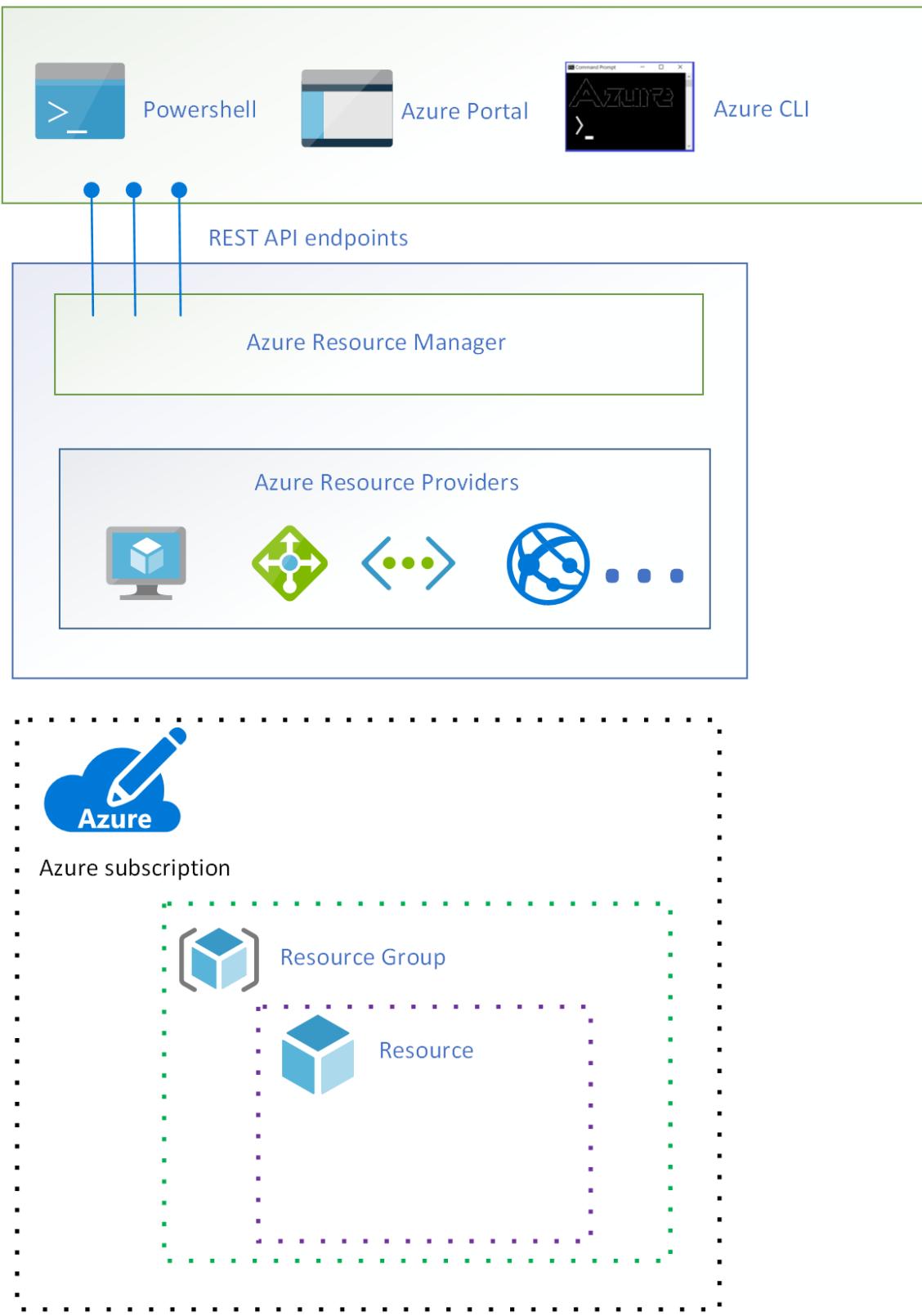


Figure 6: Azure resource providers.

When a client makes a request to manage a specific resource, Azure Resource Manager connects to the resource provider for that resource type to complete the request. For example, if a client makes a request to manage a virtual machine resource, Azure Resource Manager connects to the `Microsoft.Compute` resource provider.

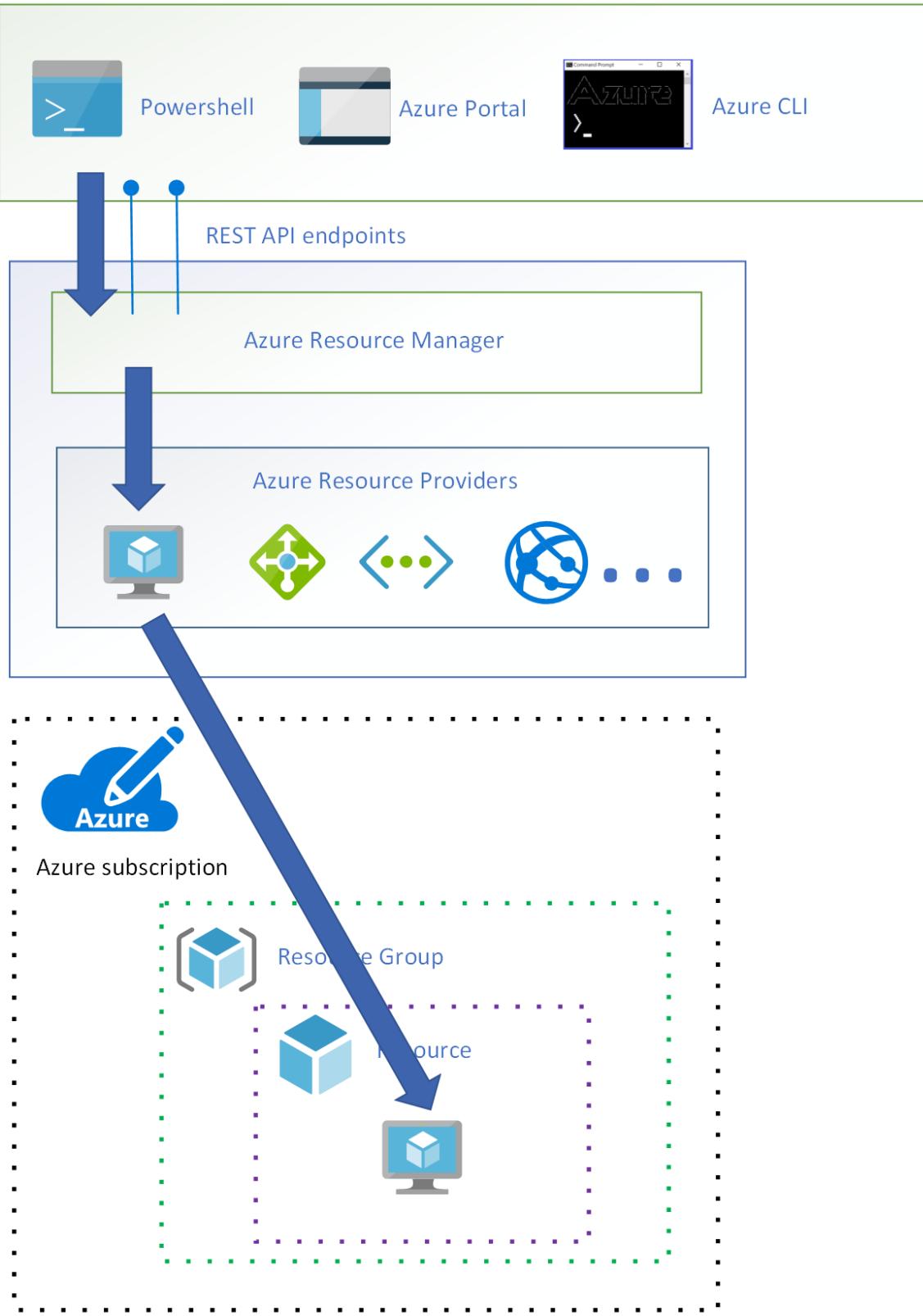


Figure 7: Azure Resource Manager connects to the `Microsoft.Compute` resource provider to manage the resource specified in the client request.

Azure Resource Manager requires the client to specify an identifier for both the subscription and the resource group in order to manage the virtual machine resource.

Now that you have an understanding of how Azure Resource Manager works, return to the discussion of how an Azure subscription is associated with the controls used by Azure Resource Manager. Before any resource management request can be executed by Azure Resource Manager, a set of controls are checked.

The first control is that a request must be made by a validated user, and Azure Resource Manager has a trusted relationship with [Azure Active Directory \(Azure AD\)](#) to provide user identity functionality.

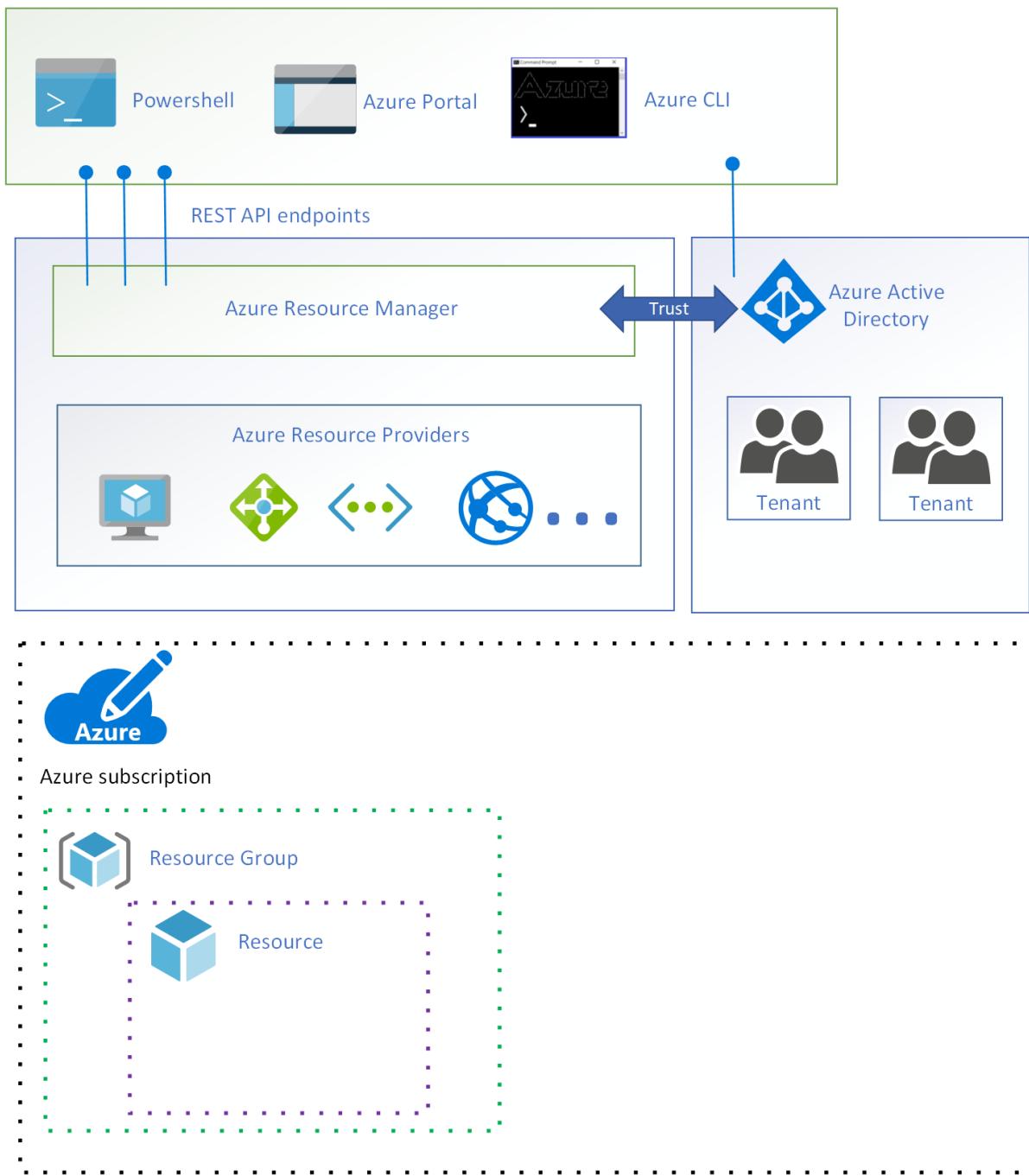


Figure 8: Azure Active Directory.

In Azure AD, users are segmented into tenants. A *tenant* is a logical construct that represents a secure, dedicated instance of Azure AD typically associated with an organization. Each subscription is associated with an Azure AD tenant.

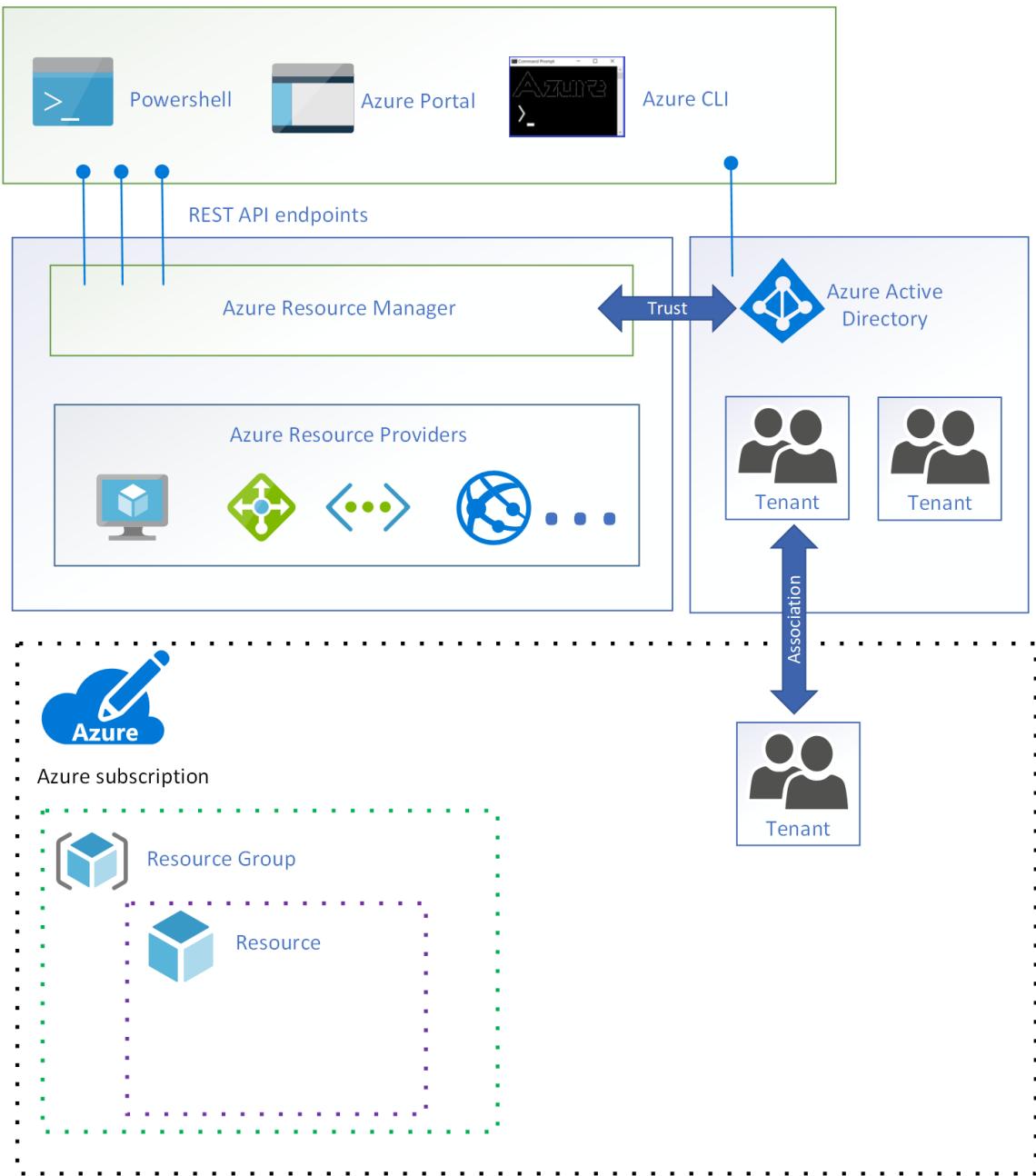


Figure 9: An Azure AD tenant associated with a subscription.

Each client request to manage a resource in a particular subscription requires that the user has an account in the associated Azure AD tenant.

The next control is a check that the user has sufficient permission to make the request. Permissions are assigned to users using [role-based access control \(RBAC\)](#).

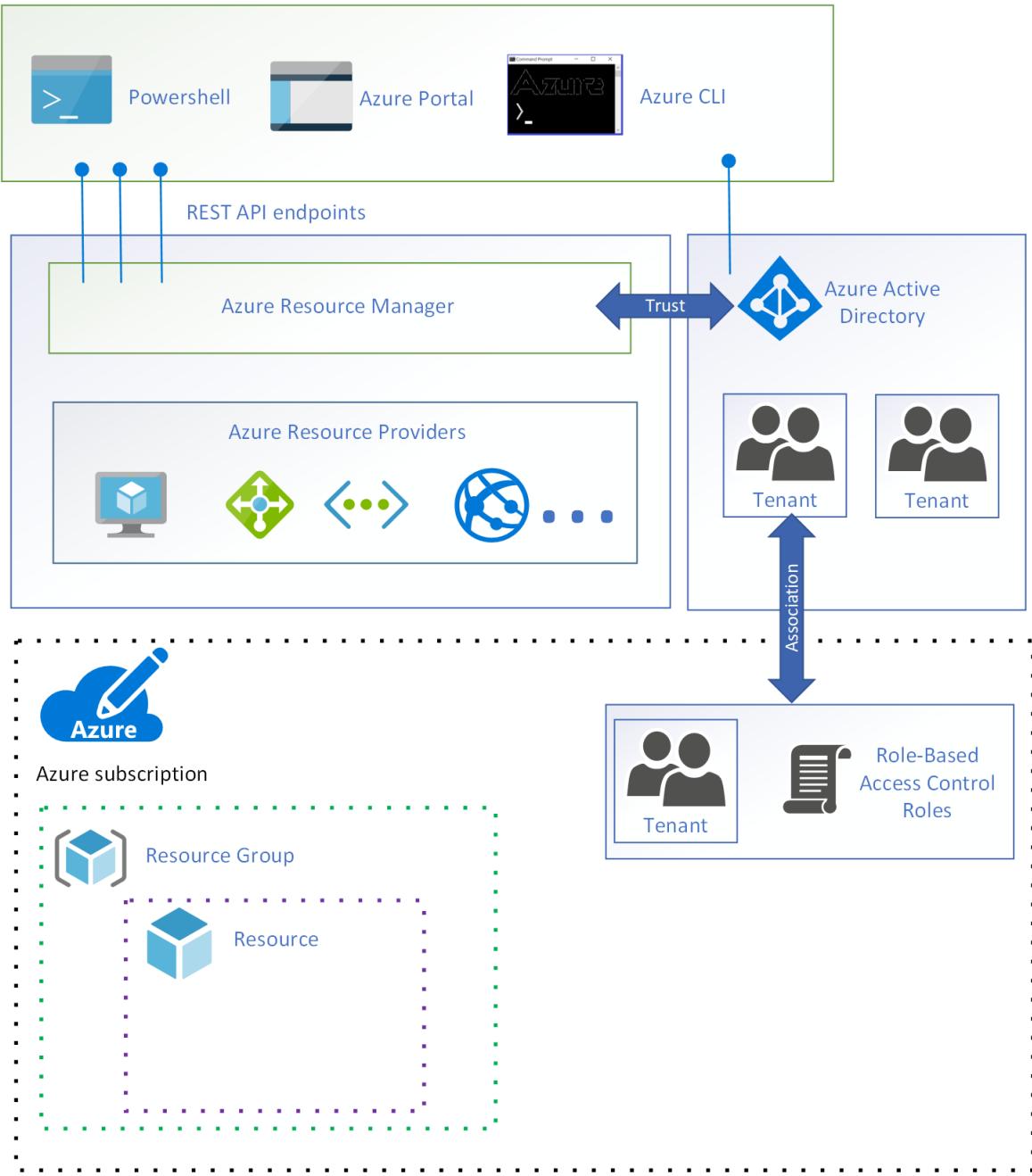


Figure 10: Each user in the tenant is assigned one or more RBAC roles.

An RBAC role specifies a set of permissions a user may take on a specific resource. When the role is assigned to the user, those permissions are applied. For example, the built-in `owner` role allows a user to perform any action on a resource.

The next control is a check that the request is allowed under the settings specified for [Azure resource policy](#). Azure resource policies specify the operations allowed for a specific resource. For example, an Azure resource policy can specify that users are only allowed to deploy a specific type of virtual machine.

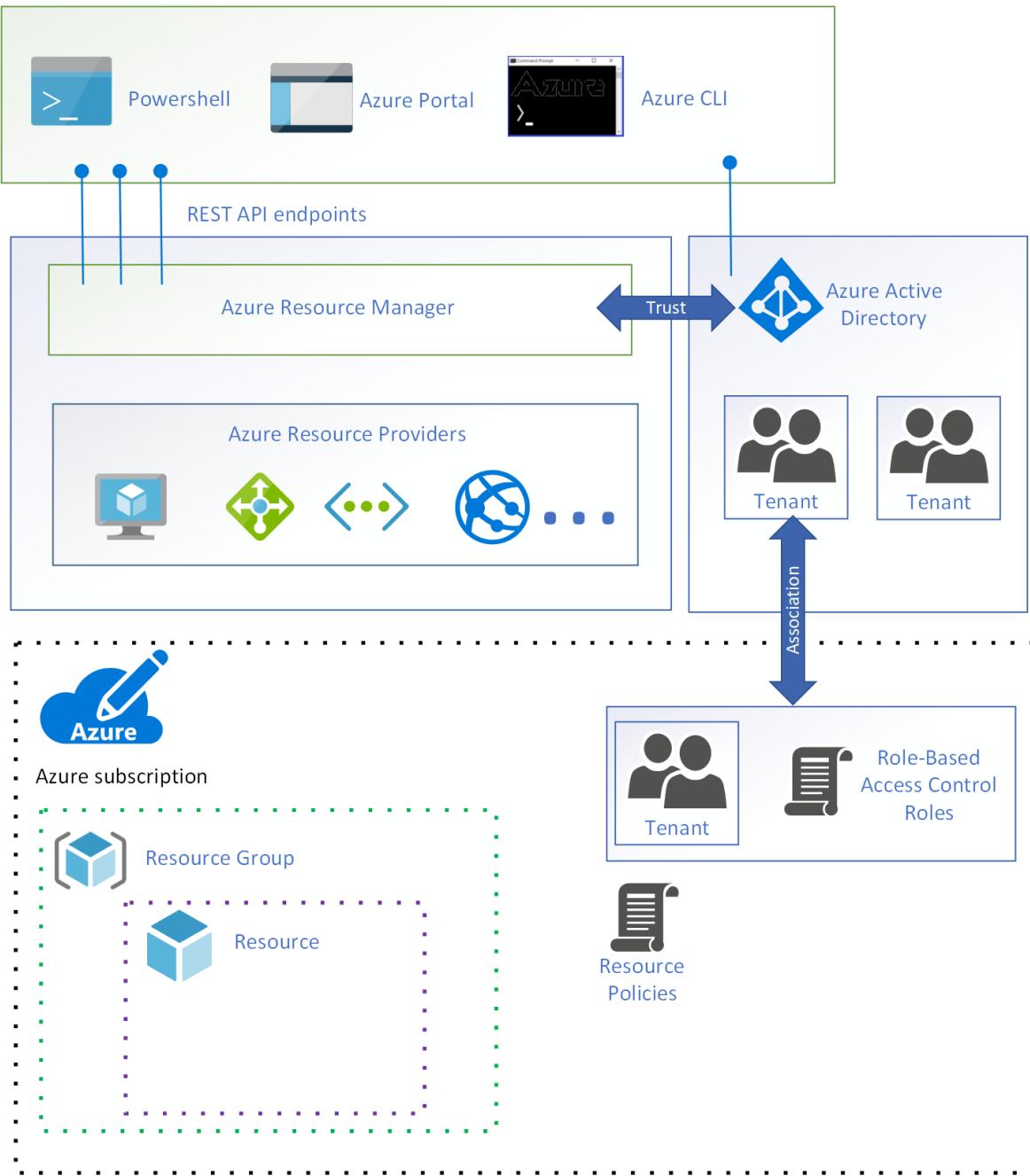


Figure 11: Azure resource policy.

The next control is a check that the request does not exceed an [Azure subscription limit](#). For example, each subscription has a limit of 980 resource groups per subscription. If a request is received to deploy an additional resource group when the limit has been reached, it is denied.

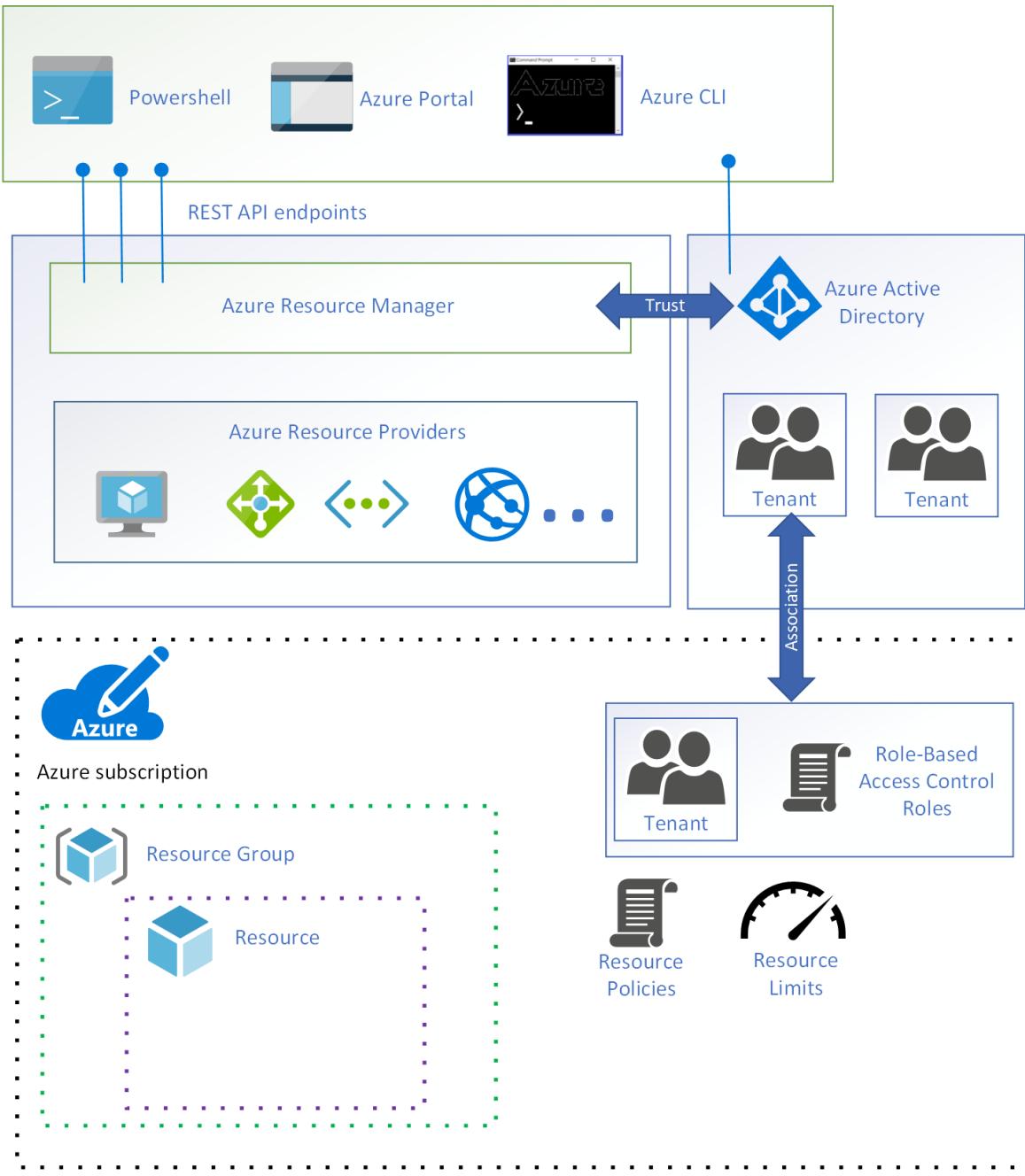


Figure 12: Azure resource limits.

The final control is a check that the request is within the financial commitment associated with the subscription. For example, if the request is to deploy a virtual machine, Azure Resource Manager verifies that the subscription has sufficient payment information.

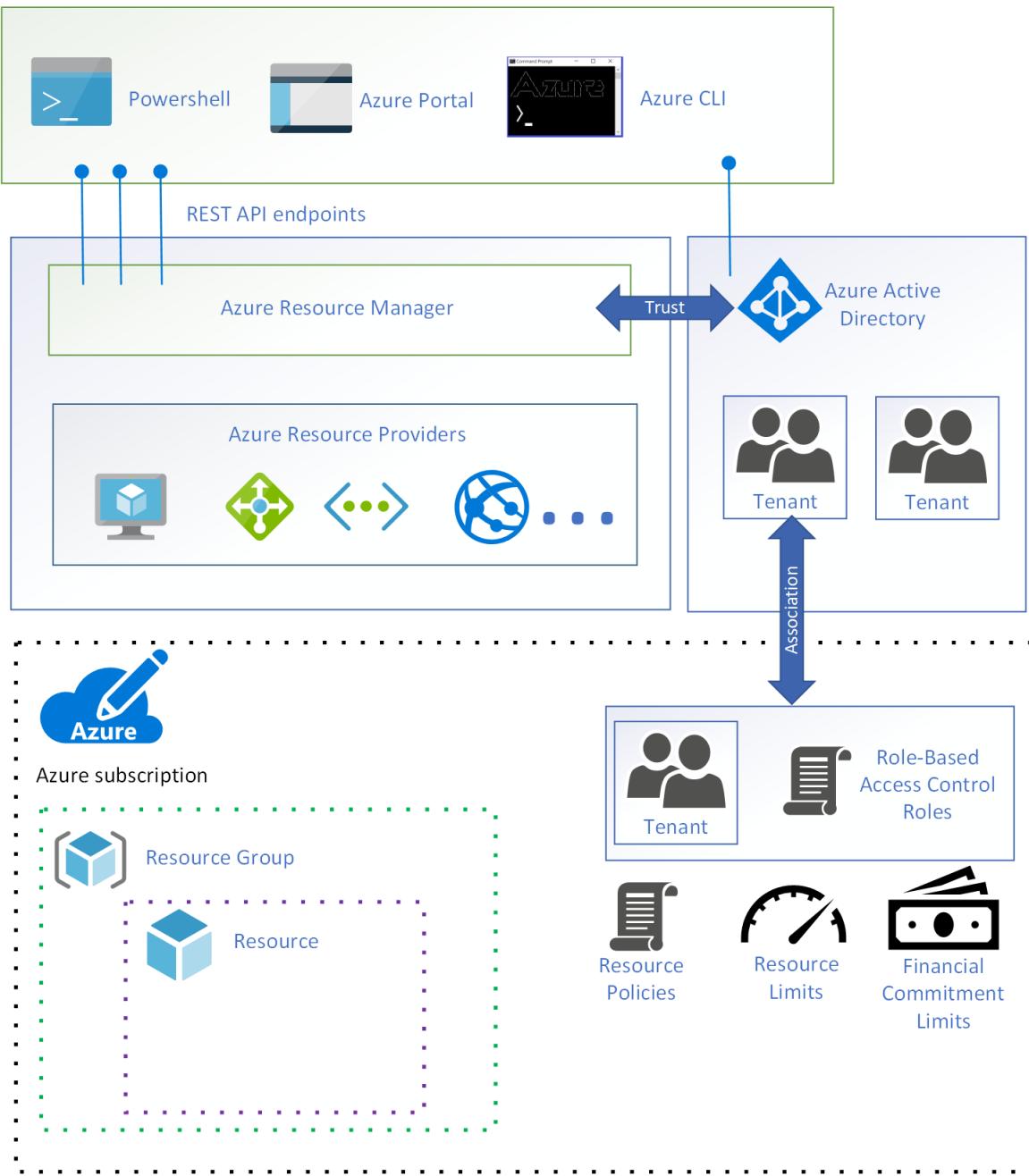


Figure 13: A financial commitment is associated with a subscription.

## Summary

In this article, you learned about how resource access is managed in Azure using Azure Resource Manager.

## Next steps

Now that you understand how to manage resource access in Azure, move on to learn how to design a governance model for a simple workload or for multiple teams using these services.

[An overview of governance](#)

# Governance design for a simple workload

11/9/2020 • 6 minutes to read • [Edit Online](#)

The goal of this guidance is to help you learn the process for designing a resource governance model in Azure to support a single team and a simple workload. You'll look at a set of hypothetical governance requirements, then go through several example implementations that satisfy those requirements.

In the foundational adoption stage, our goal is to deploy a simple workload to Azure. This results in the following requirements:

- Identity management for a single **workload owner** who is responsible for deploying and maintaining the simple workload. The workload owner requires permission to create, read, update, and delete resources as well as permission to delegate these rights to other users in the identity management system.
- Manage all resources for the simple workload as a single management unit.

## Azure licensing

Before you begin designing our governance model, it's important to understand how Azure is licensed. This is because the administrative accounts associated with your Azure license have the highest level of access to your Azure resources. These administrative accounts form the basis of your governance model.

### NOTE

If your organization has an existing [Microsoft Enterprise Agreement](#) that does not include Azure, Azure can be added by making an upfront monetary commitment. For more information, see [Licensing Azure for the enterprise](#).

When Azure was added to your organization's Enterprise Agreement, your organization was prompted to create an **Azure account**. During the account creation process, an **Azure account owner** was created, as well as an Azure Active Directory (Azure AD) tenant with a **global administrator** account. An Azure AD tenant is a logical construct that represents a secure, dedicated instance of Azure AD.

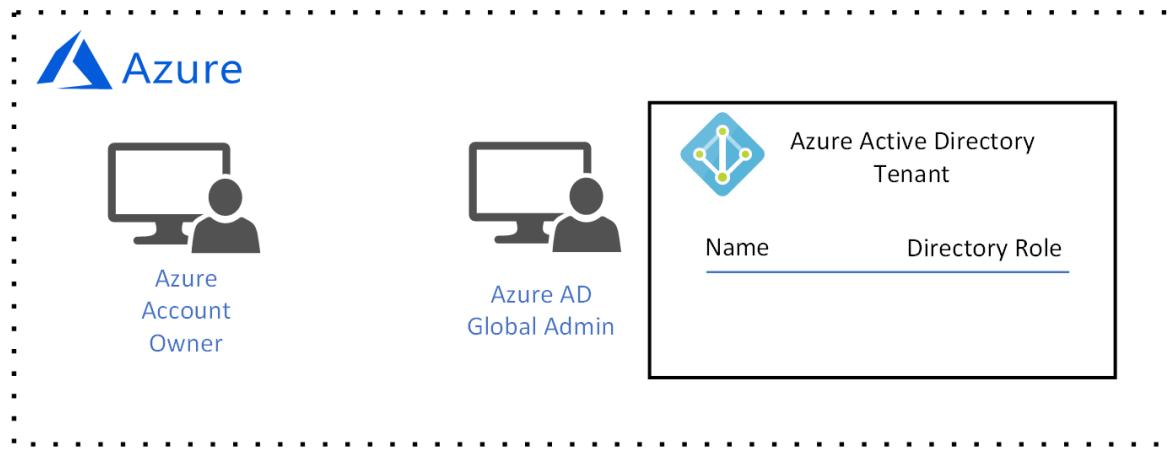


Figure 1: An Azure account with an Azure account owner and Azure AD global administrator.

## Identity management

Azure only trusts [Azure AD](#) to authenticate users and authorize user access to resources, so Azure AD is our

identity management system. The Azure AD global administrator has the highest level of permissions and can perform all actions related to identity, including creating users and assigning permissions.

Our requirement is identity management for a single **workload owner** who is responsible for deploying and maintaining the simple workload. The workload owner requires permission to create, read, update, and delete resources as well as permission to delegate these rights to other users in the identity management system.

Our Azure AD global administrator will create the **workload owner** account for the workload owner:

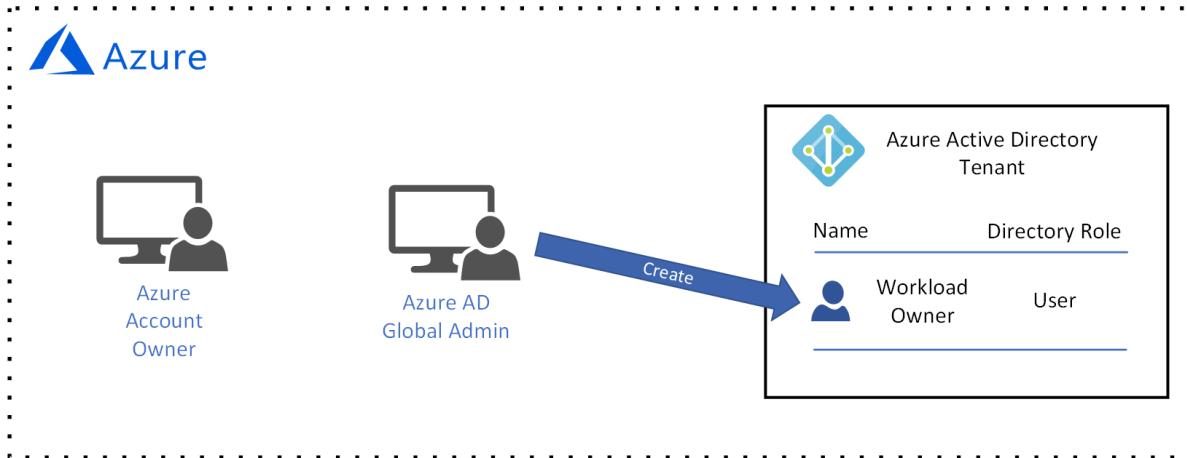


Figure 2: The Azure AD global administrator creates the workload owner user account.

You can't assign resource access permission until this user is added to a **subscription**, so you'll do that in the next two sections.

## Resource management scope

As the number of resources deployed by your organization grows, the complexity of governing those resources grows as well. Azure implements a logical container hierarchy to enable your organization to manage your resources in groups at various levels of granularity, also known as **scope**.

The top level of resource management scope is the **subscription** level. A subscription is created by the Azure **account owner**, who establishes the financial commitment and is responsible for paying for all Azure resources associated with the subscription:

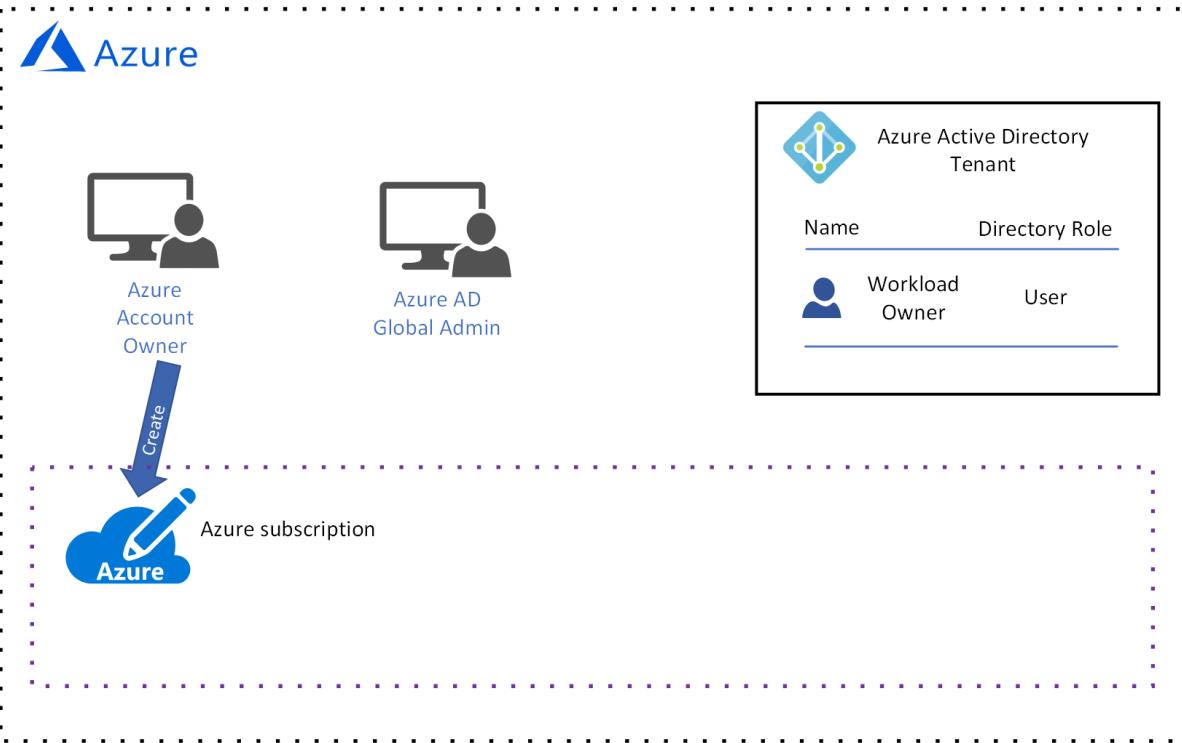


Figure 3: The Azure account owner creates a subscription.

When the subscription is created, the Azure **account owner** associates an Azure AD tenant with the subscription, and this Azure AD tenant is used for authenticating and authorizing users:

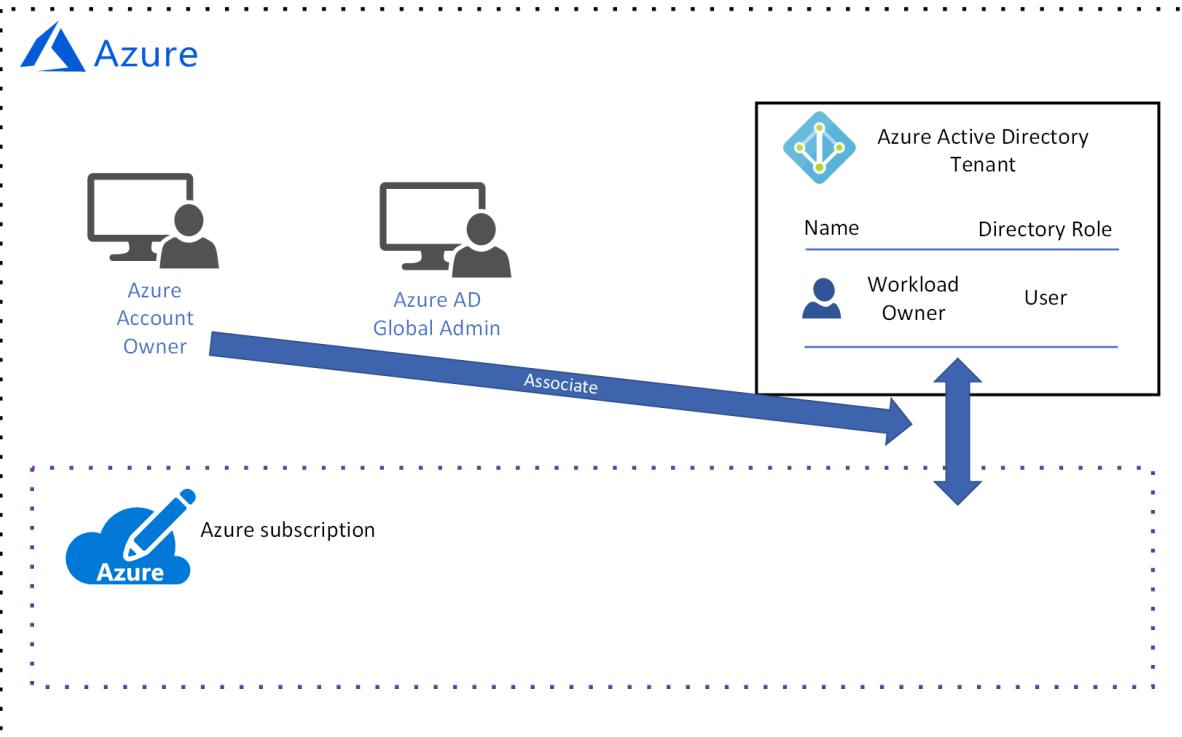


Figure 4: The Azure account owner associates the Azure AD tenant with the subscription.

You may have noticed that there is currently no user associated with the subscription, which means that no one has permission to manage resources. In practice, the **account owner** is the owner of the subscription and has permission to take any action on a resource in the subscription. In practical terms, the **account owner** is more than likely a finance person in your organization and is not responsible for creating, reading, updating, and deleting resources. Those tasks will be performed by the **workload owner**, so you need to add the **workload**

owner to the subscription and assign permissions.

Since the **account owner** is currently the only user with permission to add the **workload owner** to the subscription, they add the **workload owner** to the subscription:

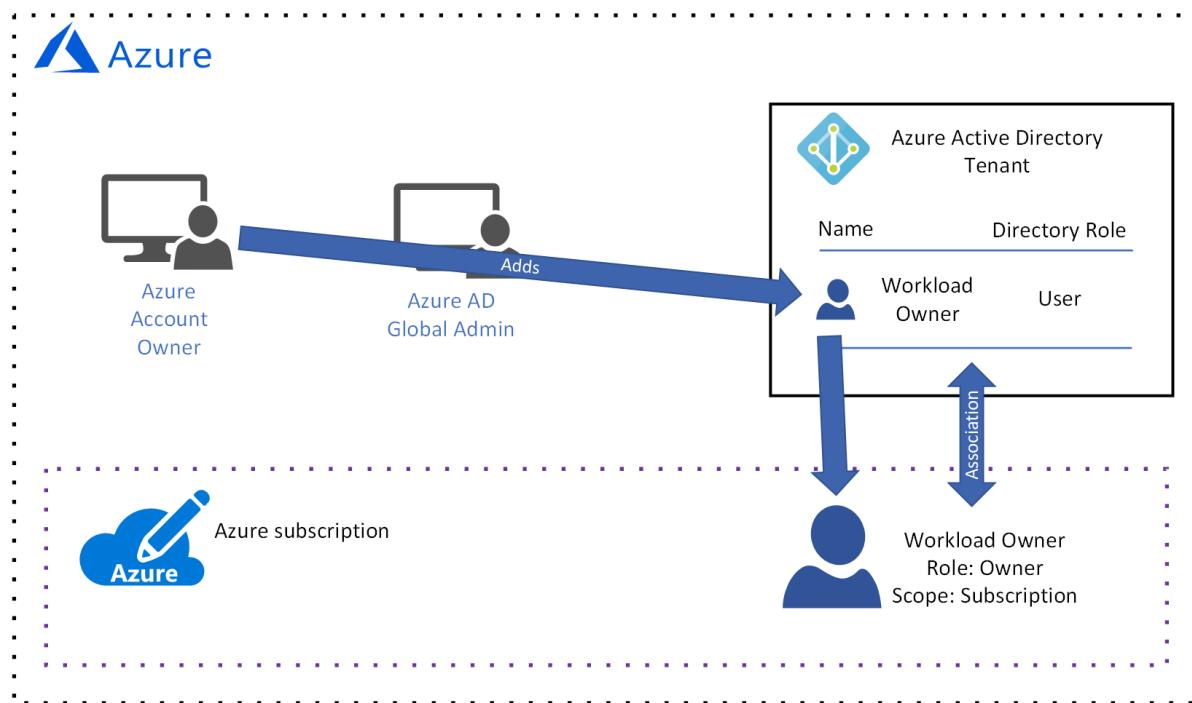


Figure 5: The Azure account owner adds the workload owner to the subscription.

The Azure **account owner** grants permissions to the **workload owner** by assigning a **role-based access control (RBAC)** role. The RBAC role specifies a set of permissions that the **workload owner** has for an individual resource type or a set of resource types.

Notice that in this example, the account owner has assigned the **built-in owner role**:

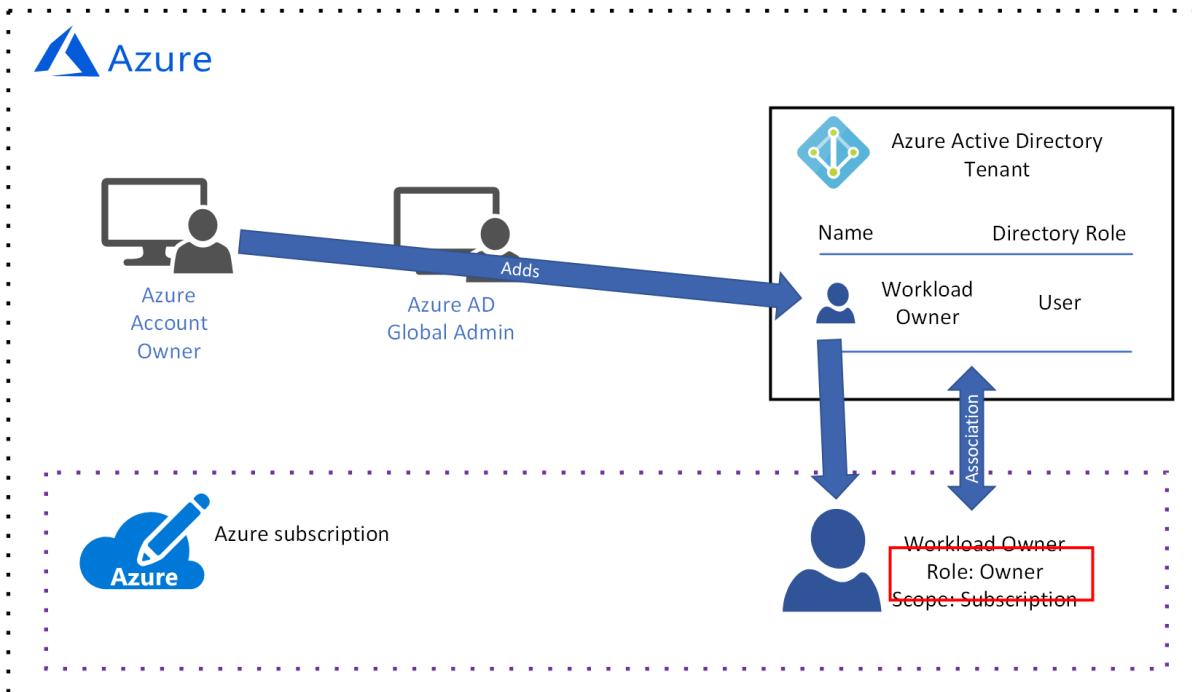


Figure 6: The workload owner was assigned the built-in owner role.

The built-in **owner** role grants all permissions to the **workload owner** at the subscription scope.

#### IMPORTANT

The Azure **account owner** is responsible for the financial commitment associated with the subscription, but the **workload owner** has the same permissions. The **account owner** must trust the **workload owner** to deploy resources that are within the subscription budget.

The next level of management scope is the **resource group** level. A resource group is a logical container for resources. Operations applied at the resource group level apply to all resources in a group. Also, it's important to note that permissions for each user are inherited from the next level up unless they're explicitly changed at that scope.

To illustrate this, let's look at what happens when the **workload owner** creates a resource group:

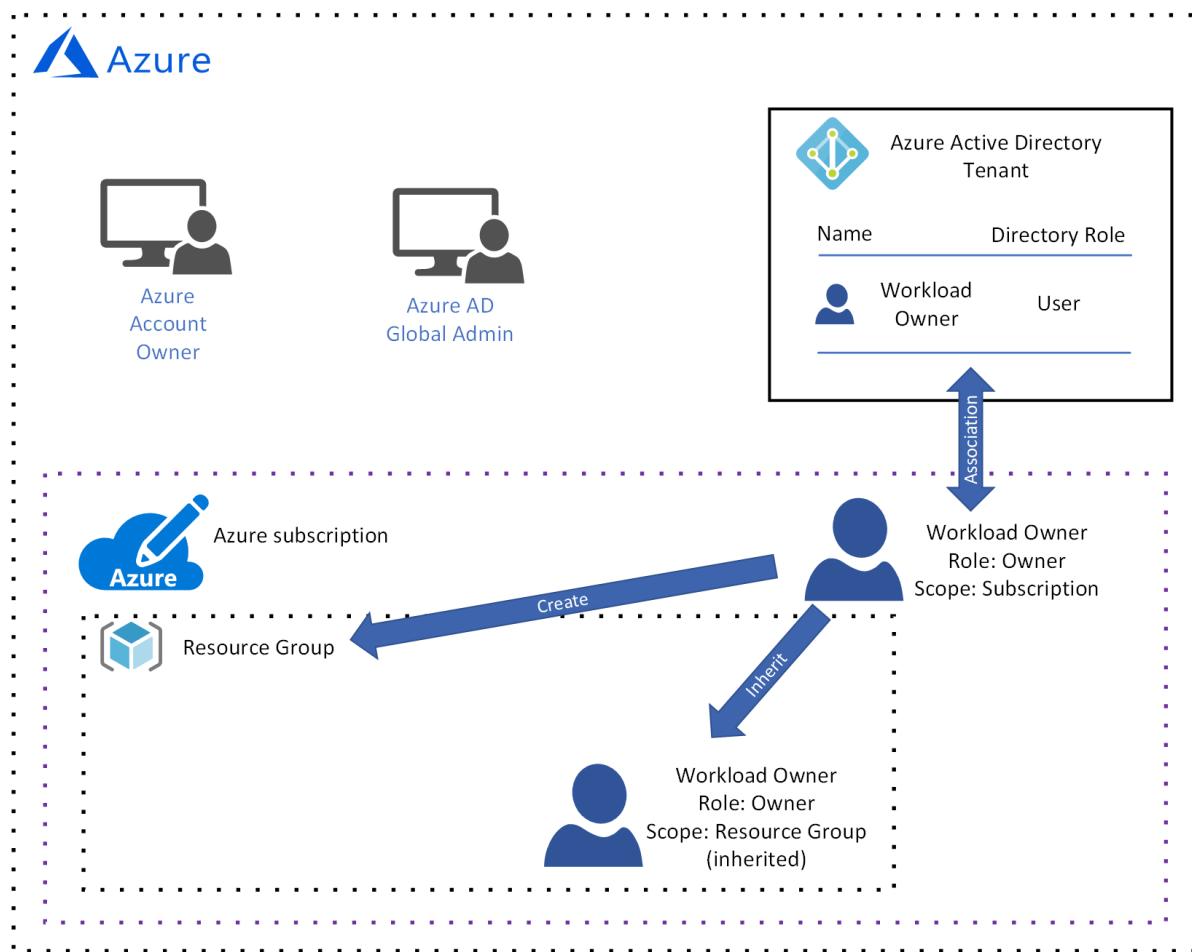


Figure 7: The workload owner creates a resource group and inherits the built-in owner role at the resource group scope.

Again, the built-in **owner** role grants all permissions to the **workload owner** at the resource group scope. As discussed earlier, this role is inherited from the subscription level. If a different role is assigned to this user at this scope, it applies to this scope only.

The lowest level of management scope is at the **resource** level. Operations applied at the resource level apply only to the resource itself. Again, permissions at the resource level are inherited from resource group scope. For example, let's look at what happens if the **workload owner** deploys a **virtual network** into the resource group:

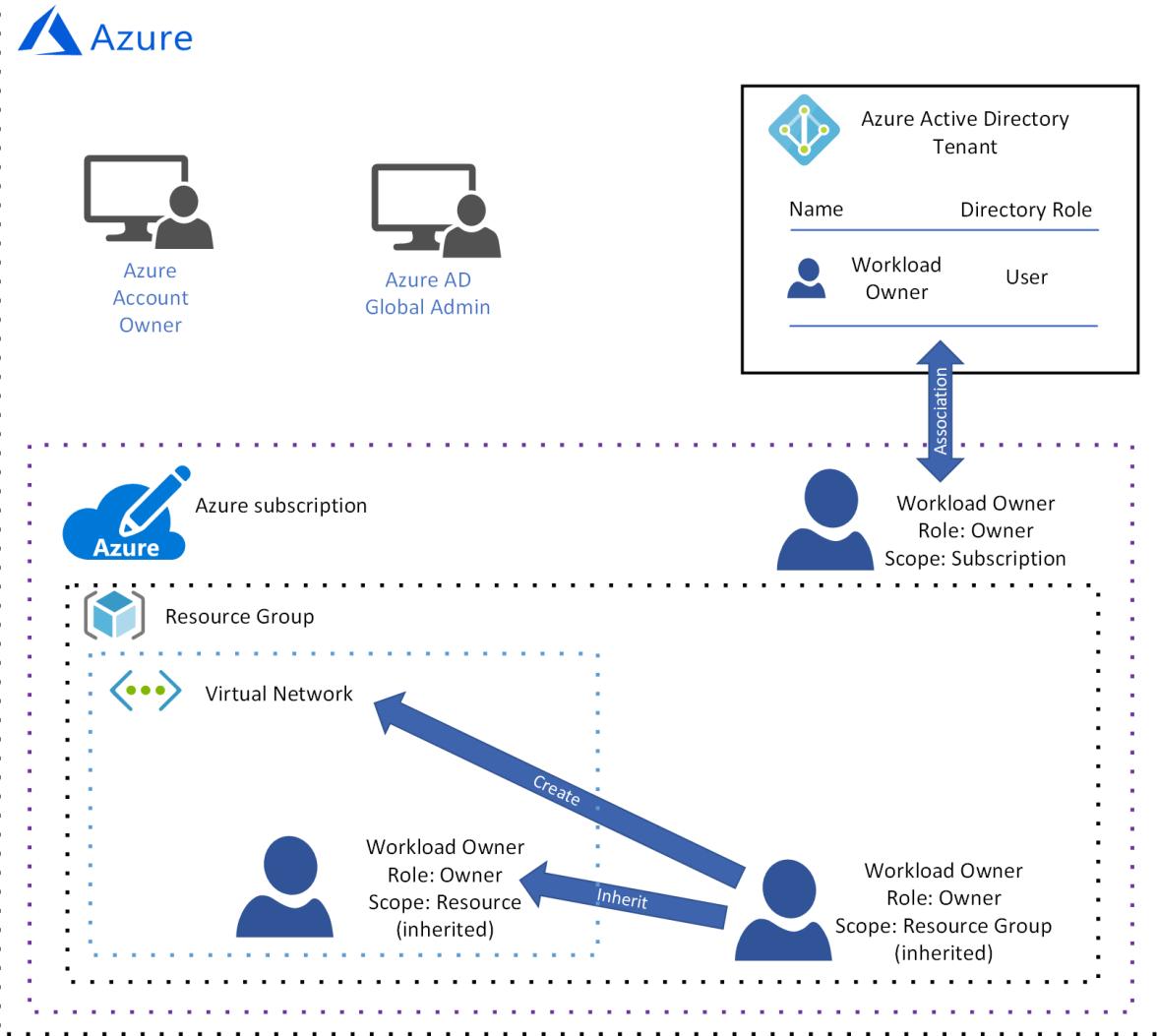


Figure 8: The workload owner creates a resource and inherits the built-in owner role at the resource scope.

The **workload owner** inherits the owner role at the resource scope, which means the workload owner has all permissions for the virtual network.

## Implement the basic resource access management model

Let's move on to learn how to implement the governance model designed earlier.

To begin, your organization requires an Azure account. If your organization has an existing [Microsoft Enterprise Agreement](#) that does not include Azure, Azure can be added by making an upfront monetary commitment. For more information, see [Licensing Azure for the enterprise](#).

When your Azure account is created, you specify a person in your organization to be the **Azure account owner**. An Azure Active Directory (Azure AD) tenant is then created by default. Your Azure **account owner** must [create the user account](#) for the person in your organization who is the **workload owner**.

Next, your Azure **account owner** must [create a subscription](#) and [associate the Azure AD tenant](#) with it.

Finally, now that the subscription is created and your Azure AD tenant is associated with it, you can [add the workload owner to the subscription with the built-in owner role](#).

## Next steps

[Learn about resource access for multiple teams](#)

# Governance design for multiple teams

11/9/2020 • 24 minutes to read • [Edit Online](#)

The goal of this guidance is to help you learn the process for designing a resource governance model in Azure to support multiple teams, multiple workloads, and multiple environments. First you'll look at a set of hypothetical governance requirements, then go through several example implementations that satisfy those requirements.

The requirements are:

- The enterprise plans to transition new cloud roles and responsibilities to a set of users and therefore requires identity management for multiple teams with different resource access needs in Azure. This identity management system is required to store the identity of the following users:
  - The individual in your organization responsible for ownership of **subscriptions**.
  - The individual in your organization responsible for the **shared infrastructure resources** used to connect your on-premises network to a virtual network in Azure.
  - Two individuals in your organization responsible for managing a **workload**.
- Support for multiple **environments**. An environment is a logical grouping of resources, such as virtual machines, virtual networking, and network traffic routing services. These groups of resources have similar management and security requirements and are typically used for a specific purpose such as testing or production. In this example, the requirement is for four environments:
  - A **shared infrastructure environment** that includes resources shared by workloads in other environments. For example, a virtual network with a gateway subnet that provides connectivity to on-premises.
  - A **production environment** with the most restrictive security policies. Could include internal or external facing workloads.
  - A **nonproduction environment** for development and testing work. This environment has security, compliance, and cost policies that differ from those in the production environment. In Azure, this takes the form of an Enterprise Dev/Test subscription.
  - A **sandbox environment** for proof of concept and education purposes. This environment is typically assigned per employee participating in development activities and has strict procedural and operational security controls in place to prevent corporate data from landing here. In Azure, these take the form of Visual Studio subscriptions. These subscriptions should also *not* be tied to the enterprise Azure Active Directory.
- A **permissions model of least privilege** in which users have no permissions by default. The model must support the following:
  - A single trusted user at the subscription scope, treated like a service account and granted permission to assign resource access rights.
  - Each workload owner is denied access to resources by default. Resource access rights are granted explicitly by the single trusted user at the resource group scope.
  - Management access for the shared infrastructure resources, limited to the shared infrastructure owners.
  - Management access for each workload restricted to the workload owner in production, and increasing levels of control as development proceeds through the various deployment environments (development, test, staging, and production).
  - The enterprise does not want to have to manage roles independently in each of the three main environments, and therefore requires the use of only **built-in roles** available in Azure's role-based access control (RBAC). If the enterprise absolutely requires custom RBAC roles, additional processes would be needed to synchronize custom roles across the three environments.

- Cost tracking by workload owner name, environment, or both.

## Identity management

Before you can design identity management for your governance model, it's important to understand the four major areas it encompasses:

- **Administration:** The processes and tools for creating, editing, and deleting user identity.
- **Authentication:** Verifying user identity by validating credentials, such as a user name and password.
- **Authorization:** Determining which resources an authenticated user is allowed to access or what operations they have permission to perform.
- **Auditing:** Periodically reviewing logs and other information to discover security issues related to user identity. This includes reviewing suspicious usage patterns, periodically reviewing user permissions to verify they're accurate, and other functions.

There is only one service trusted by Azure for identity, and that is Azure Active Directory (Azure AD). You'll be adding users to Azure AD and using it for all of the functions listed above. Before looking at how to configure Azure AD, it's important to understand the privileged accounts that are used to manage access to these services.

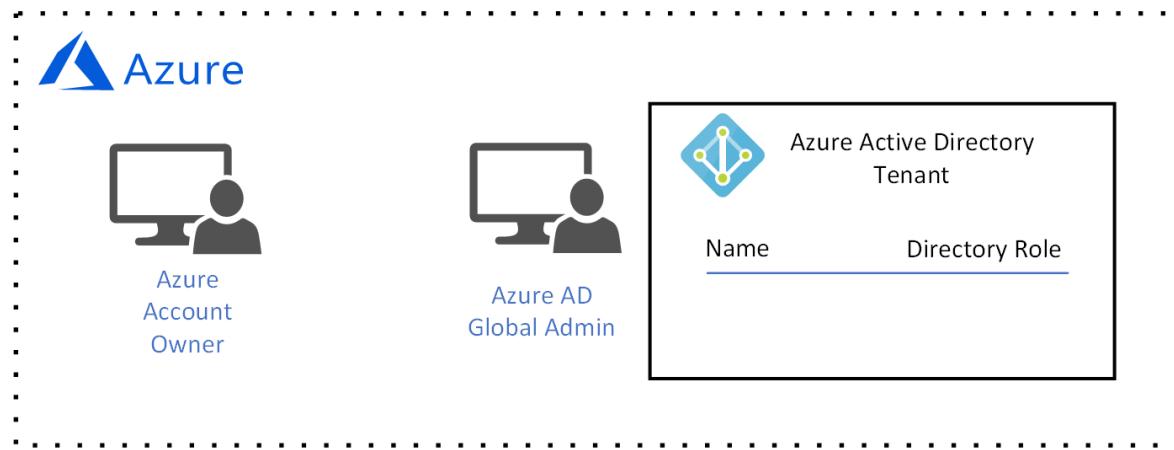
When your organization signed up for an Azure account, at least one Azure **account owner** was assigned. Also, an Azure AD **tenant** was created, unless an existing tenant was already associated with your organization's use of other Microsoft services such as Microsoft 365. A **global administrator** with full permissions on the Azure AD tenant was associated when it was created.

The user identities for both the Azure account owner and the Azure AD global administrator are stored in a highly secure identity system that is managed by Microsoft. The Azure account owner is authorized to create, update, and delete subscriptions. The Azure AD global administrator is authorized to perform many actions in Azure AD, but for this design guide you'll focus on the creation and deletion of user identity.

### NOTE

Your organization may already have an existing Azure AD tenant if there's an existing Microsoft 365, Intune, or Dynamics 365 license associated with your account.

The Azure account owner has permission to create, update, and delete subscriptions:



*Figure 1: An Azure account with an Azure account owner and Azure AD global administrator.*

The Azure AD **global administrator** has permission to create user accounts:

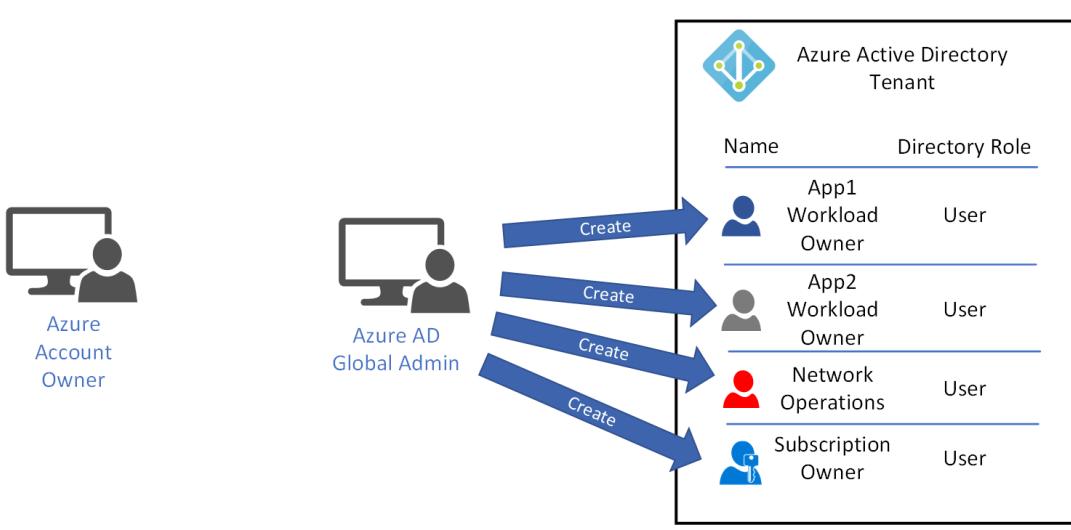


Figure 2: The Azure AD global administrator creates the required user accounts in the tenant.

The first two accounts, **app1 workload owner** and **app2 workload owner**, are each associated with an individual in your organization responsible for managing a workload. The **network operations** account is owned by the individual that is responsible for the shared infrastructure resources. Finally, the **subscription owner** account is associated with the individual responsible for ownership of subscriptions.

## Resource access permissions model of least privilege

Now that your identity management system and user accounts have been created, you have to decide how to apply role-based access control (RBAC) roles to each account to support a permissions model of least privilege.

There's another requirement stating the resources associated with each workload be isolated from one another such that no one workload owner has management access to any other workload they do not own. There's also a requirement to implement this model using only built-in roles for Azure role-based access control.

Each RBAC role is applied at one of three scopes in Azure: **subscription**, **resource group**, then an individual **resource**. Roles are inherited at lower scopes. For example, if a user is assigned the **built-in owner role** at the subscription level, that role is also assigned to that user at the resource group and individual resource level unless overridden.

Therefore, to create a model of least-privilege access you have to decide the actions a particular type of user is allowed to take at each of these three scopes. For example, the requirement is for a workload owner to have permission to manage access to only the resources associated with their workload and no others. If you were to assign the built-in owner role at the subscription scope, each workload owner would have management access to all workloads.

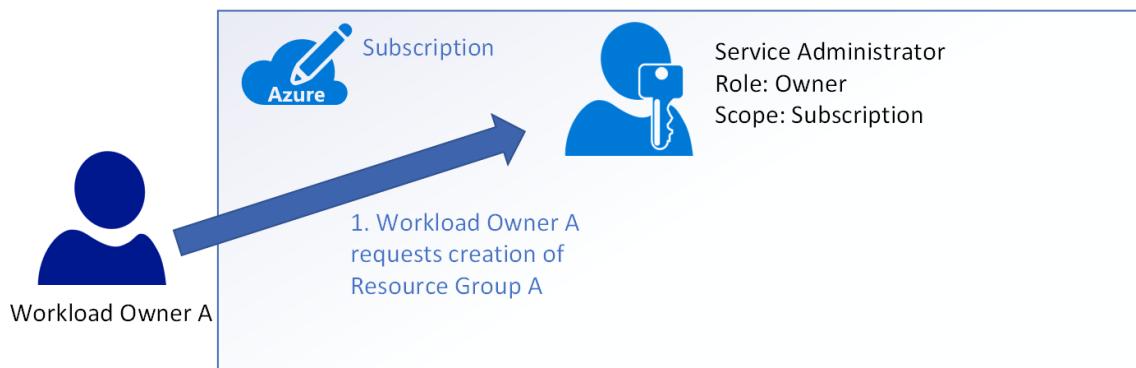
Let's take a look at two example permission models to understand this concept a little better. In the first example, the model trusts only the service administrator to create resource groups. In the second example, the model assigns the built-in owner role to each workload owner at the subscription scope.

In both examples, there is a subscription service administrator that is assigned the built-in owner role at the subscription scope. Recall that the built-in owner role grants all permissions including the management of access to resources.

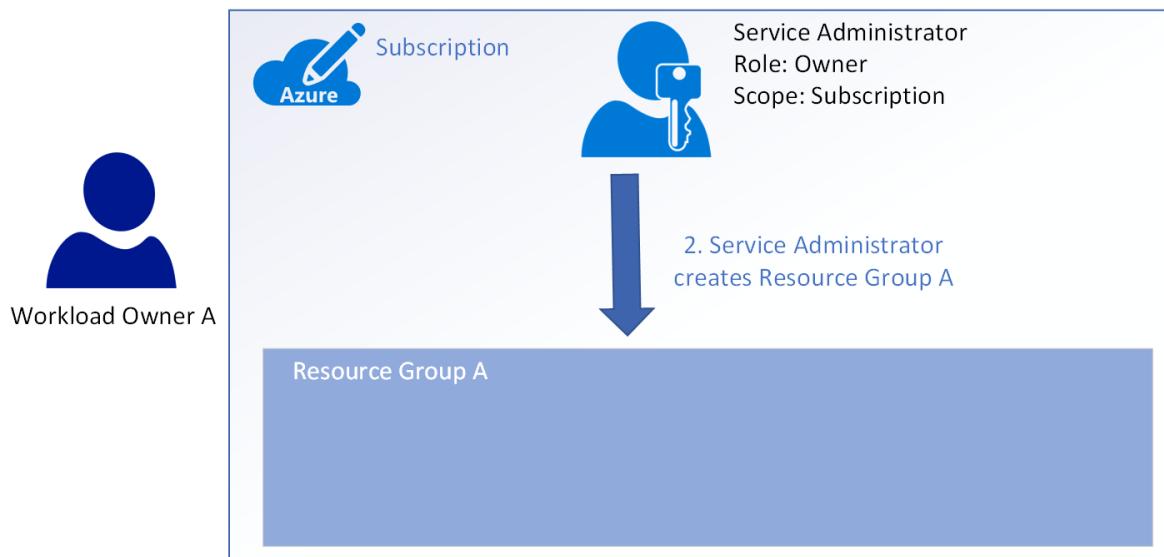


Figure 3: A subscription with a service administrator assigned the built-in owner role.

1. In the first example, **workload owner A** has no permissions at the subscription scope and no resource access management rights by default. This user wants to deploy and manage the resources for their workload. They must contact the **service administrator** to request creation of a resource group.



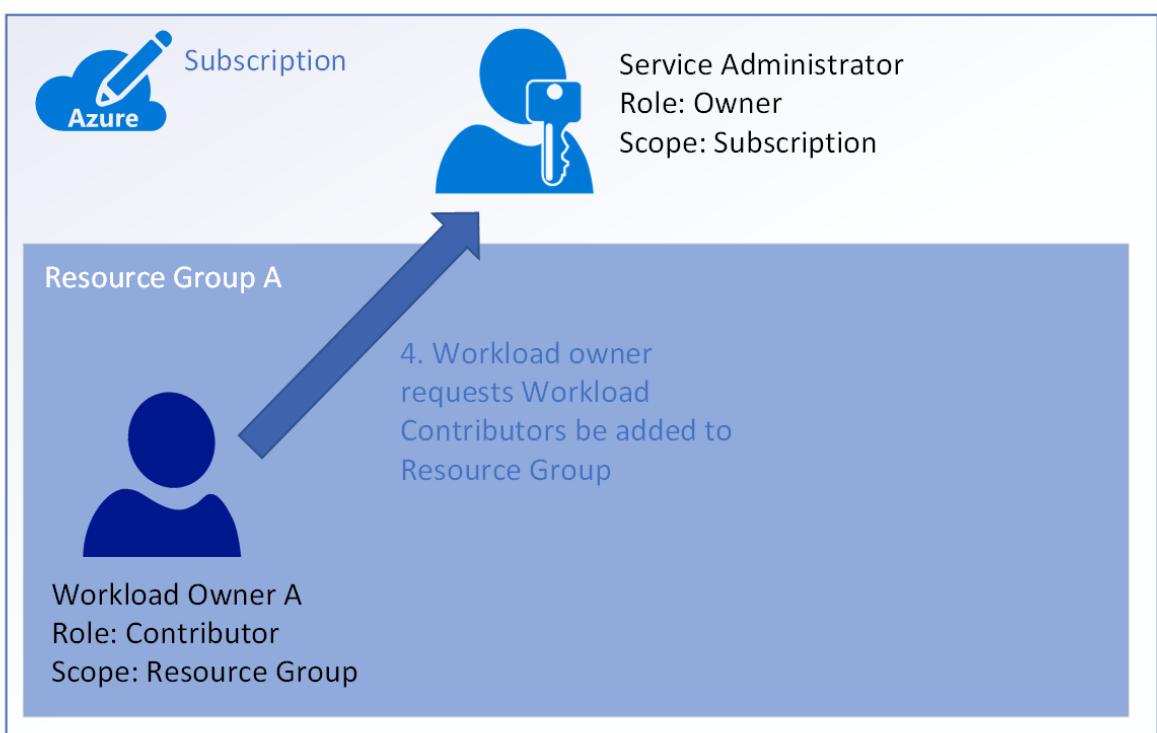
2. The **service administrator** reviews their request and creates **resource group A**. At this point, **workload owner A** still doesn't have permission to do anything.



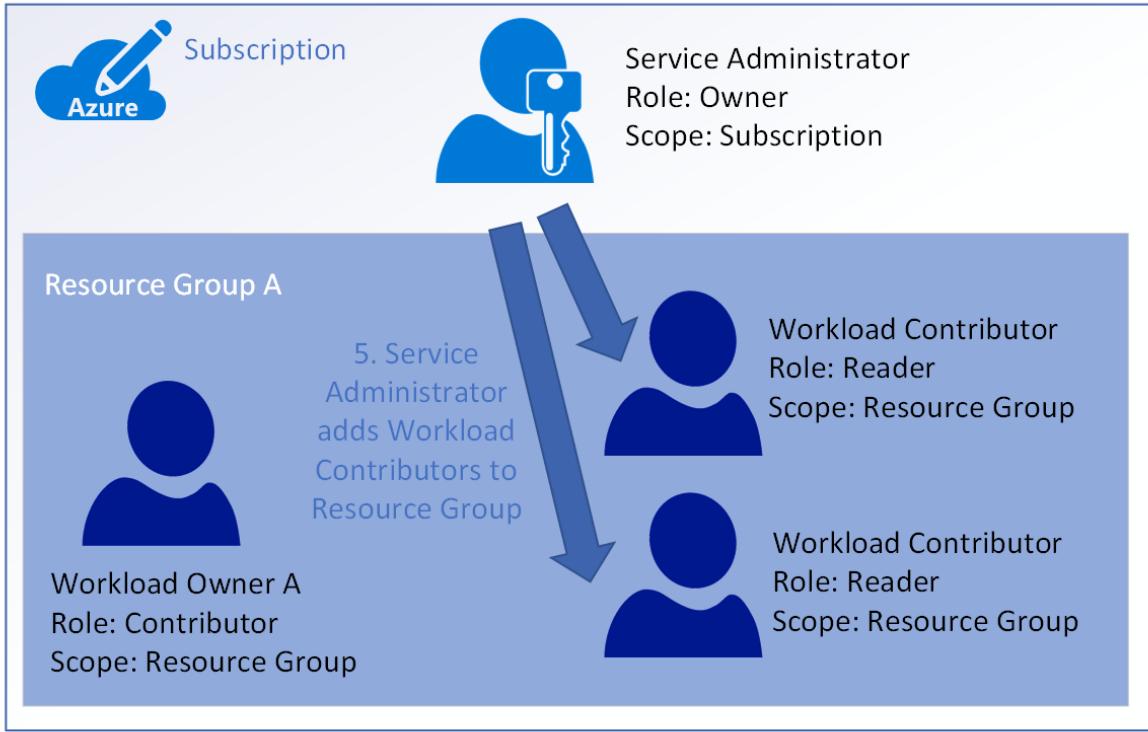
3. The **service administrator** adds **workload owner A** to **resource group A** and assigns the **built-in Contributor role**. The Contributor role grants all permissions on **resource group A** except managing access permission.



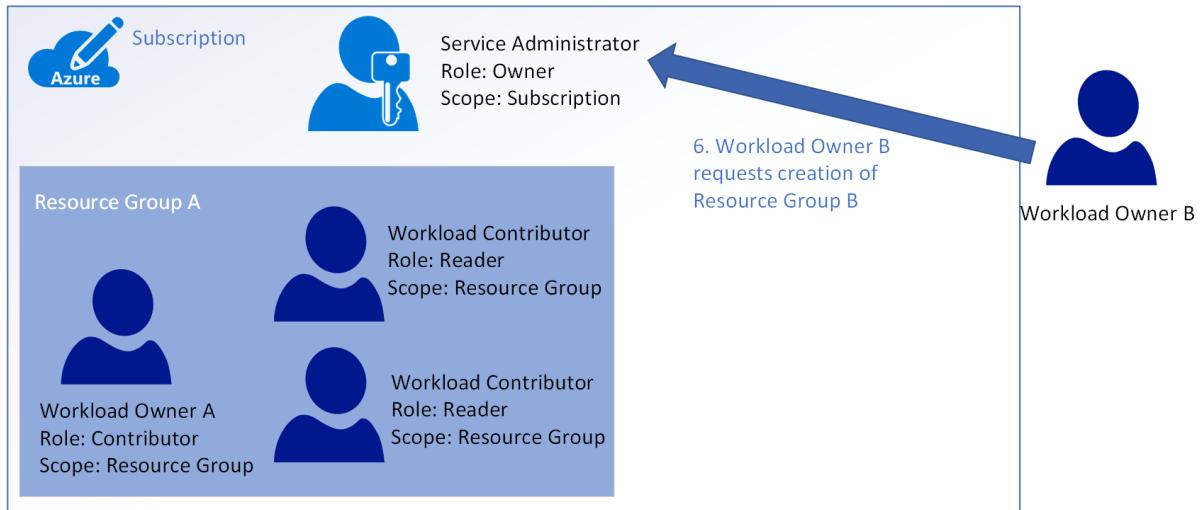
4. Let's assume that **workload owner A** has a requirement for a pair of team members to view the CPU and network traffic monitoring data as part of capacity planning for the workload. Because **workload owner A** is assigned the **Contributor** role, they do not have permission to add a user to **resource group A**. They must send this request to the **service administrator**.



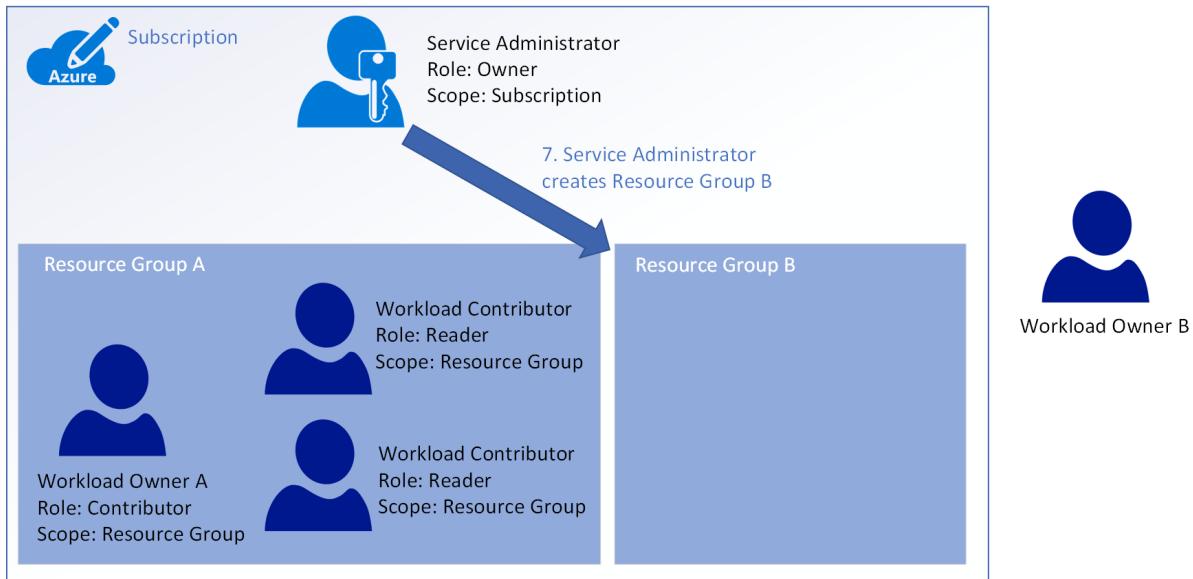
5. The **service administrator** reviews the request, and adds the two **workload contributor** users to **resource group A**. Neither of these two users require permission to manage resources, so they're assigned the **built-in reader role**.



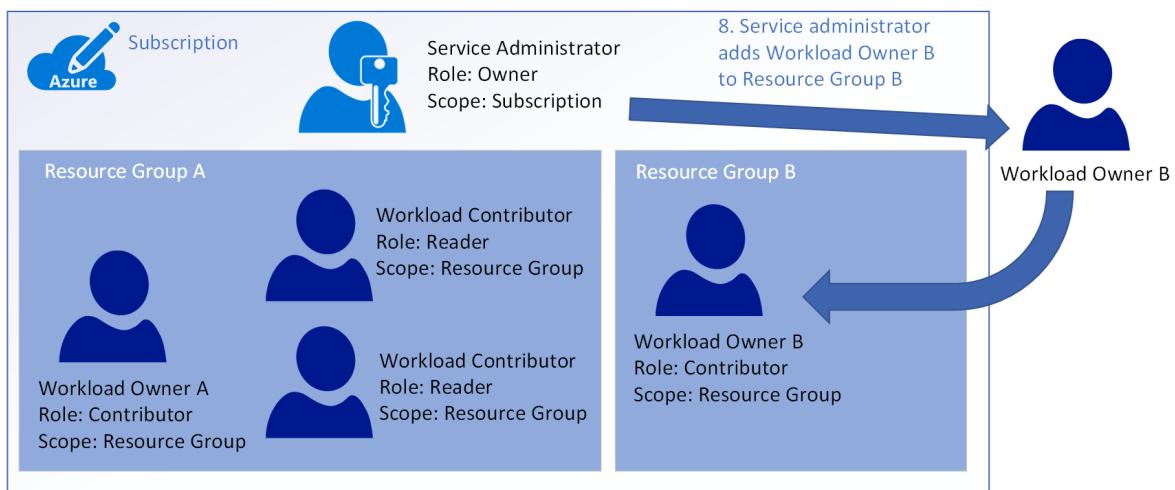
6. Next, **workload owner B** also requires a resource group to contain the resources for their workload. As with **workload owner A**, **workload owner B** initially does not have permission to take any action at the subscription scope so they must send a request to the **service administrator**.



7. The **service administrator** reviews the request and creates **resource group B**.



8. The service administrator then adds workload owner B to resource group B and assigns the built-in Contributor role.



At this point, each of the workload owners is isolated in their own resource group. None of the workload owners or their team members have management access to the resources in any other resource group.

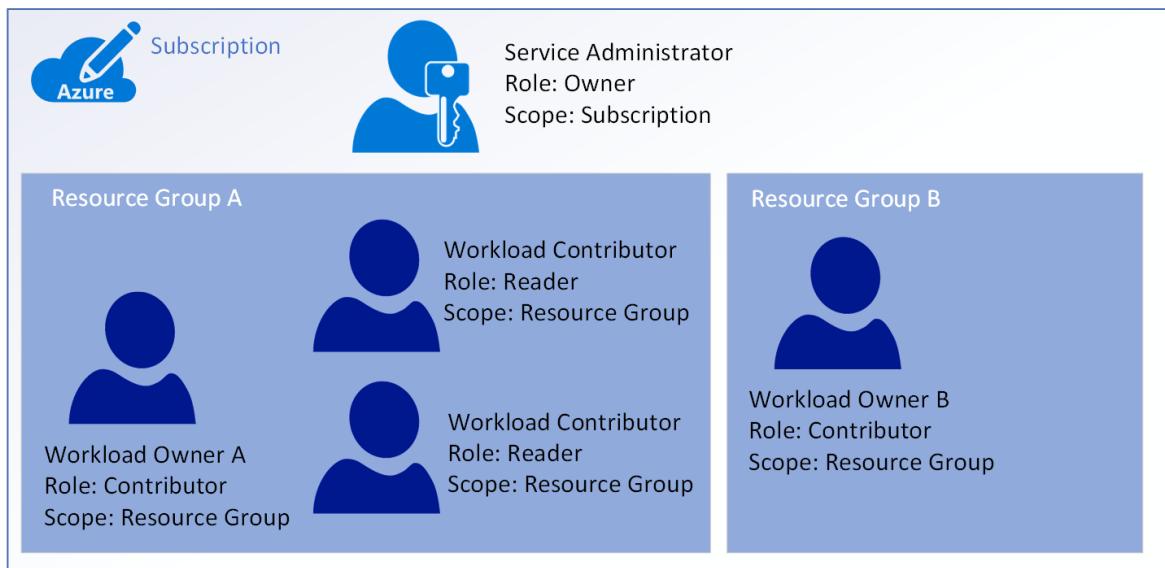


figure 4: a subscription with two workload owners isolated with their own resource group.\_

This model is a least-privilege model. Each user is assigned the correct permission at the correct resource management scope.

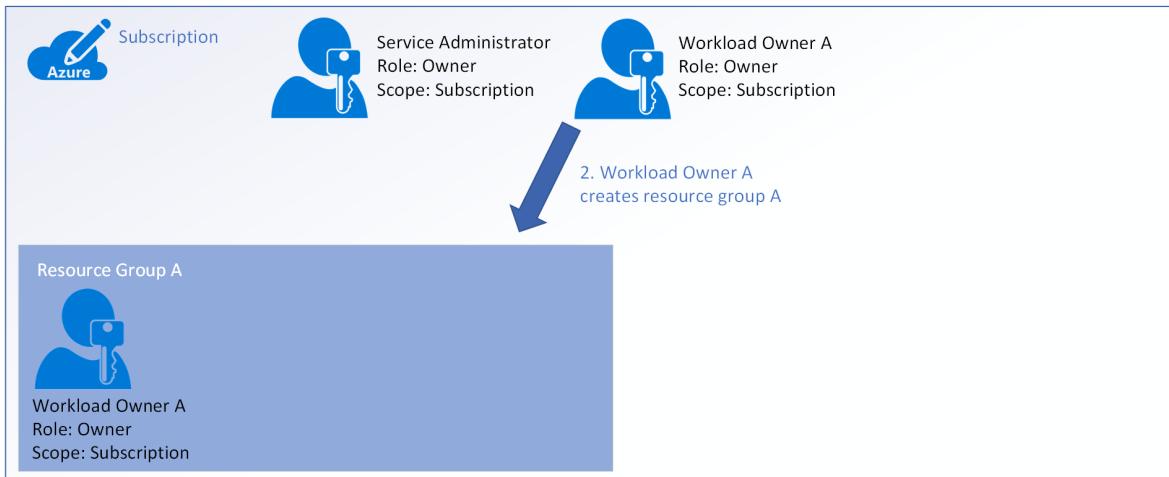
Consider that every task in this example was performed by the **service administrator**. While this is a simple example and may not appear to be an issue because there were only two workload owners, it's easy to imagine the types of issues that would result for a large organization. For example, the **service administrator** can become a bottleneck with a large backlog of requests that result in delays.

Let's take a look at second example that reduces the number of tasks performed by the **service administrator**.

1. In this model, **workload owner A** is assigned the built-in owner role at the subscription scope, enabling them to create their own resource group: **resource group A**.

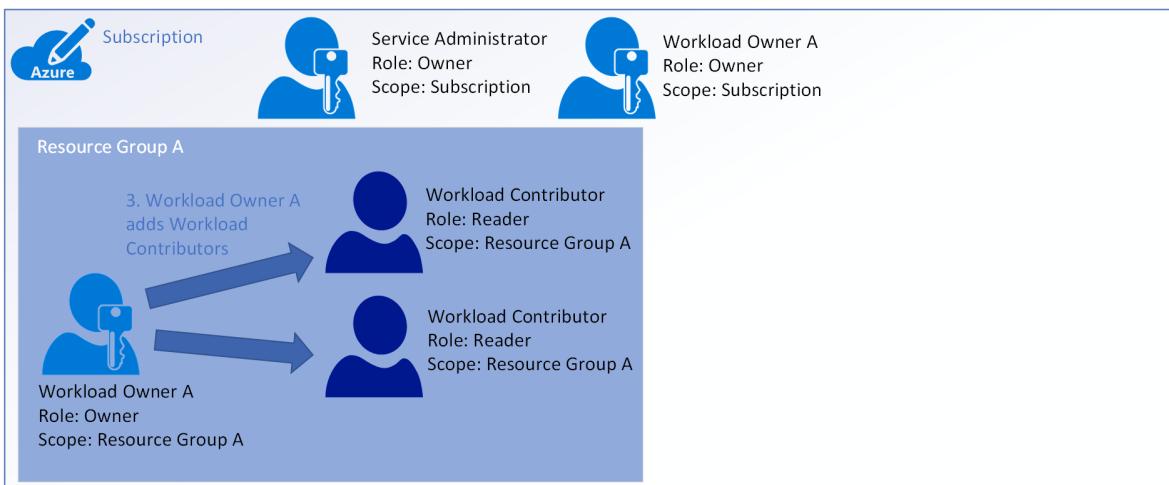


2. When **resource group A** is created, **workload owner A** is added by default and inherits the built-in owner role from the subscription scope.

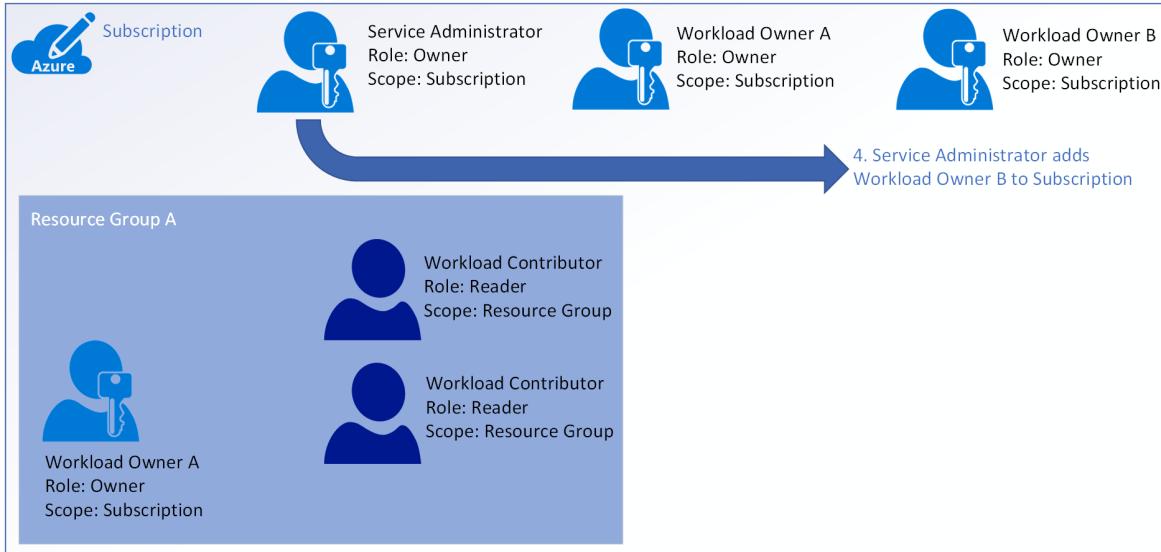


3. The built-in owner role grants **workload owner A** permission to manage access to the resource group.

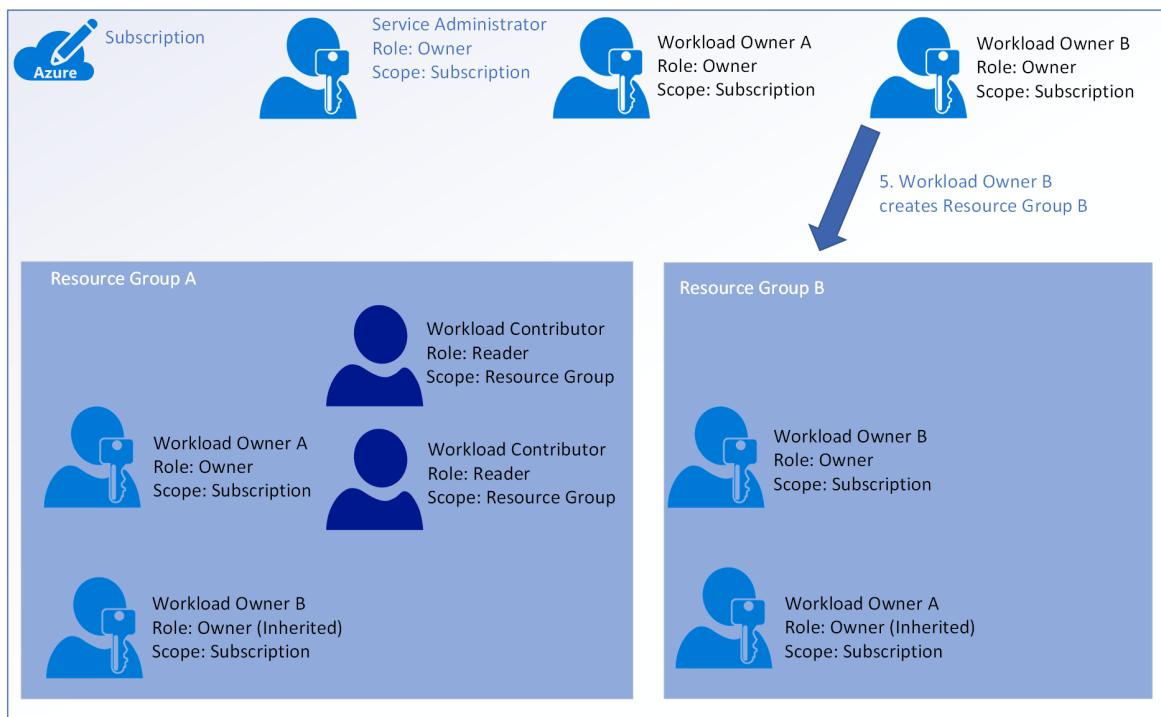
**Workload owner A** adds two **workload contributors** and assigns the built-in reader role to each of them.



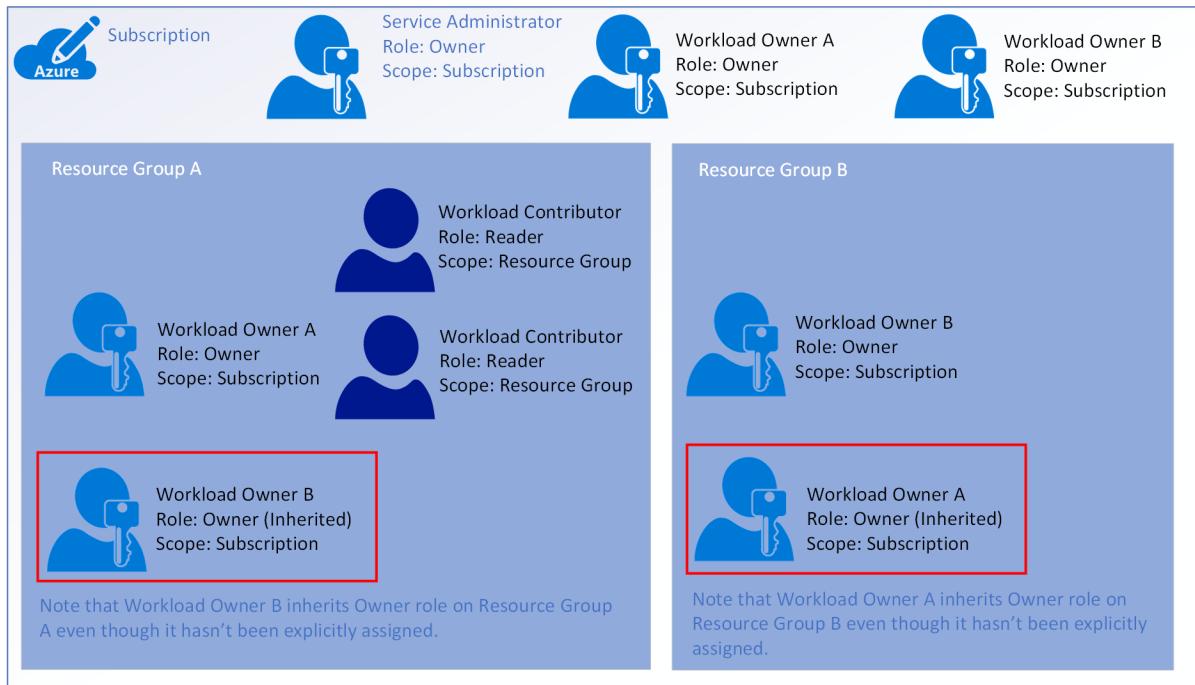
4. Service administrator now adds **workload owner B** to the subscription with the built-in owner role.



5. **Workload owner B creates resource group B** and is added by default. Again, **workload owner B** inherits the built-in owner role from the subscription scope.



Note that in this model, the **service administrator** performed fewer actions than they did in the first example due to the delegation of management access to each of the individual workload owners.



*Figure 5: A subscription with a service administrator and two workload owners, all assigned the built-in owner role.*

Because both **workload owner A** and **workload owner B** are assigned the built-in owner role at the subscription scope, they have each inherited the built-in owner role for each other's resource group. This means that not only do they have full access to each other's resources, they can also delegate management access to each other's resource groups. For example, **workload owner B** has rights to add any other user to **resource group A** and can assign any role to them, including the built-in owner role.

If you compare each example to the requirements, you'll see that both examples support a single trusted user at the subscription scope with permission to grant resource access rights to the two workload owners. Each of the two workload owners did not have access to resource management by default and required the **service administrator** to explicitly assign permissions to them. Only the first example supports the requirement that the resources associated with each workload are isolated from one another such that no workload owner has access to the resources of any other workload.

## Resource management model

Now that you've designed a permissions model of least privilege, let's move on to take a look at some practical applications of these governance models. Recall from the requirements that you must support the following three environments:

1. **Shared infrastructure environment:** A group of resources shared by all workloads. These are resources such as network gateways, firewalls, and security services.
2. **Production environment:** Multiple groups of resources representing multiple production workloads. These resources are used to host the private and public-facing application artifacts. These resources typically have the tightest governance and security models to protect the resources, application code, and data from unauthorized access.
3. **Preproduction environment:** Multiple groups of resources representing multiple non-production-ready workloads. These resources are used for development and testing, and may have a more relaxed governance model to enable increased developer agility. Security within these groups should increase as the application development process moves closer to production.

For each of these three environments, there is a requirement to track cost data by **workload owner**,

**environment**, or both. That is, you'll want to know the ongoing cost of the **shared infrastructure**, the costs incurred by individuals in both the **nonproduction** and **production** environments, and finally the overall cost of **nonproduction** and **production** environments.

You have already learned that resources are scoped to two levels: **subscription** and **resource group**. Therefore, the first decision is how to organize environments by **subscription**. There are only two possibilities: a single subscription or multiple subscriptions.

Before you look at examples of each of these models, let's review the management structure for subscriptions in Azure.

Recall from the requirements that you have an individual in the organization who is responsible for subscriptions, and this user owns the **subscription owner** account in the Azure AD tenant. This account does not have permission to create subscriptions. Only the **Azure account owner** has permission to do this:

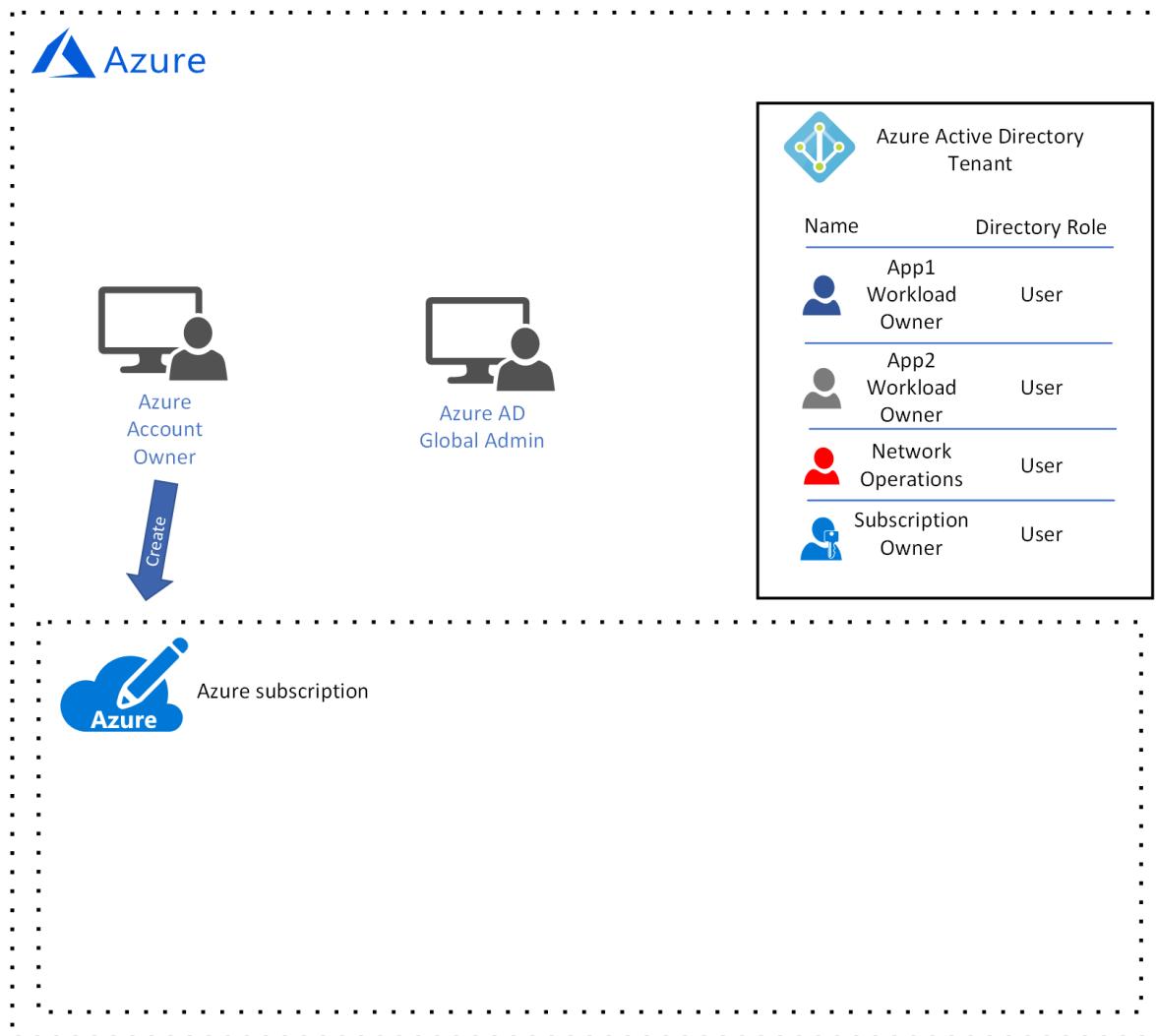


Figure 6: An Azure account owner creates a subscription.

Once the subscription has been created, the **Azure account owner** can add the **subscription owner** account to the subscription with the **owner** role:

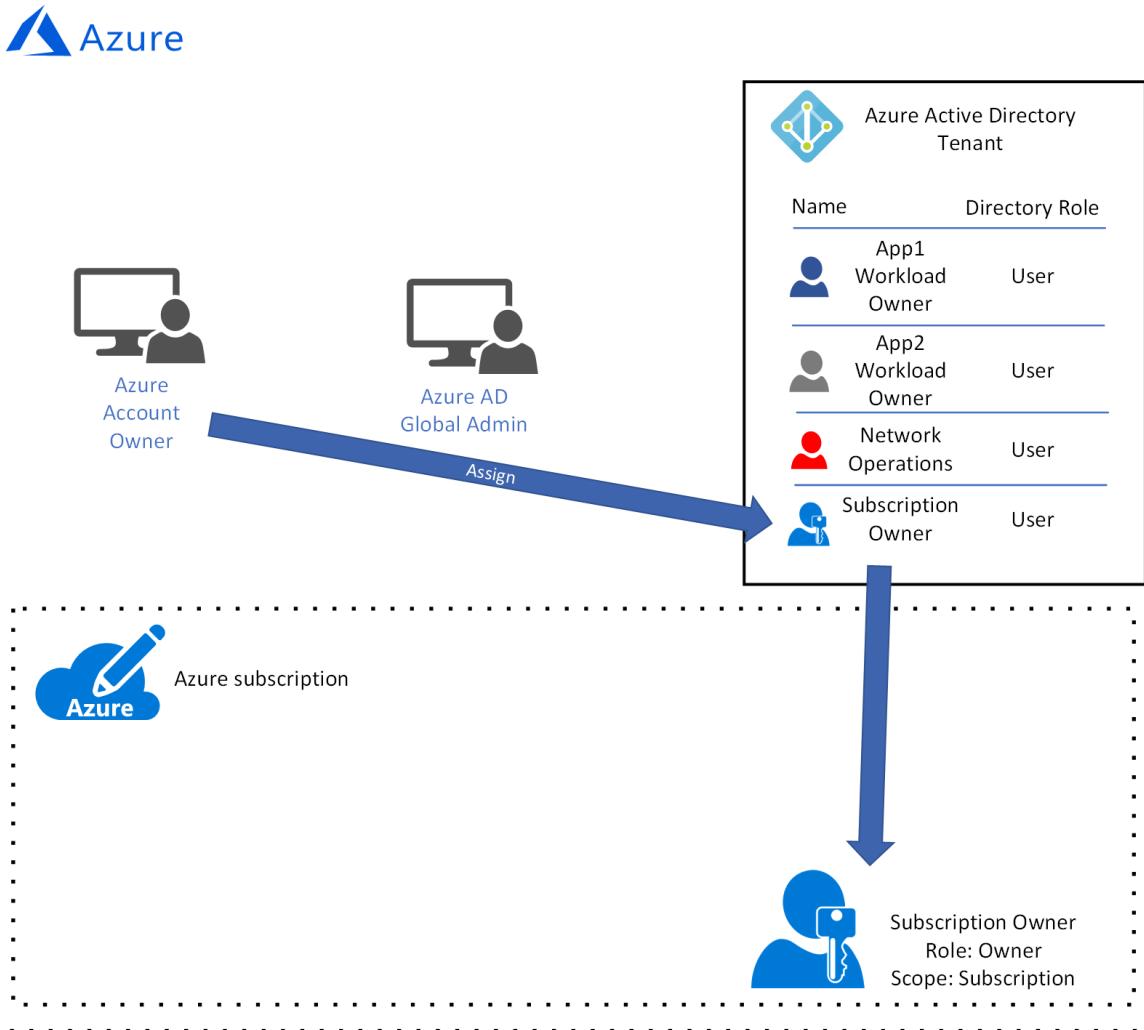


Figure 7: The Azure account owner adds the **subscription owner** user account to the subscription with the **owner** role.

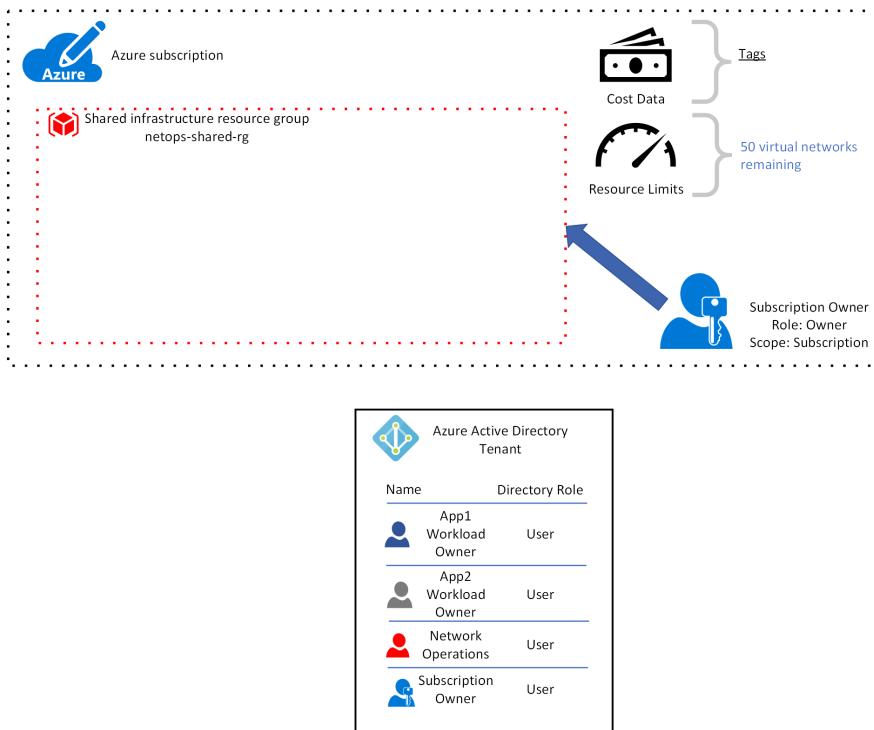
The **subscription owner** account can now create **resource groups** and delegate resource access management.

First let's look at an example resource management model using a single subscription. The first decision is how to align resource groups to the three environments. You have two options:

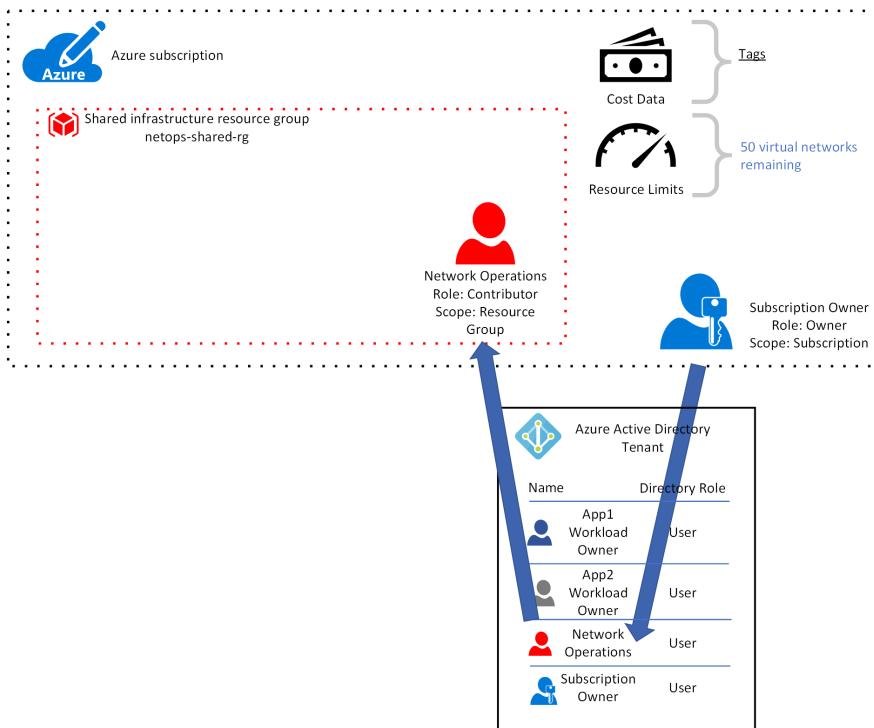
1. Align each environment to a single resource group. All shared infrastructure resources are deployed to a single **shared infrastructure** resource group. All resources associated with development workloads are deployed to a single **development** resource group. All resources associated with production workloads are deployed into a single **production** resource group for the **production** environment.
2. Create separate resource groups for each workload, using a naming convention and tags to align resource groups with each of the three environments.

Let's begin by evaluating the first option. You'll be using the permissions model that was discussed in the previous section, with a single subscription service administrator who creates resource groups and adds users to them with either the built-in **contributor** or **reader** role.

1. The first resource group deployed represents the **shared infrastructure** environment. The **subscription owner** account creates a resource group for the shared infrastructure resources named `netops-shared-rg`.

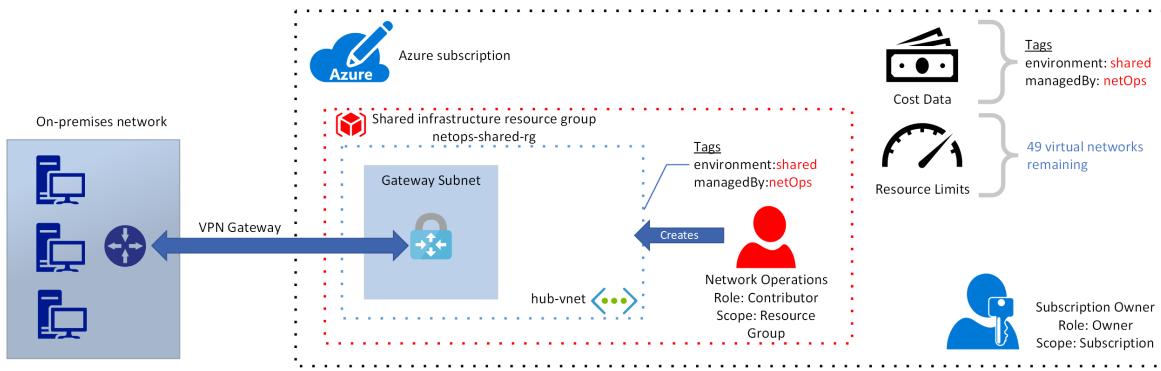


2. The **subscription owner** account adds the **network operations user** account to the resource group and assigns the **contributor** role.

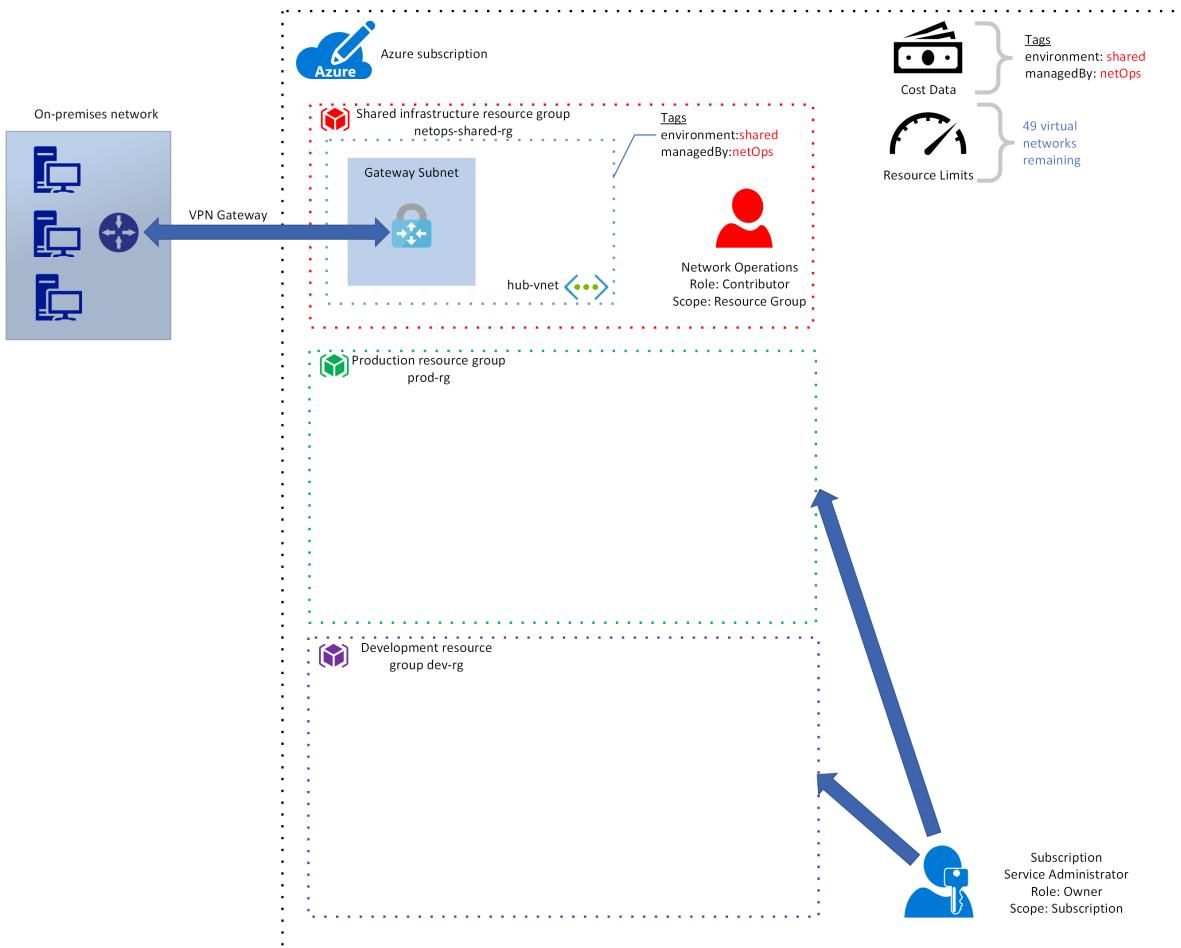


3. The **network operations user** creates a **VPN gateway** and configures it to connect to the on-premises VPN appliance. The **network operations user** also applies a pair of **tags** to each of the resources:

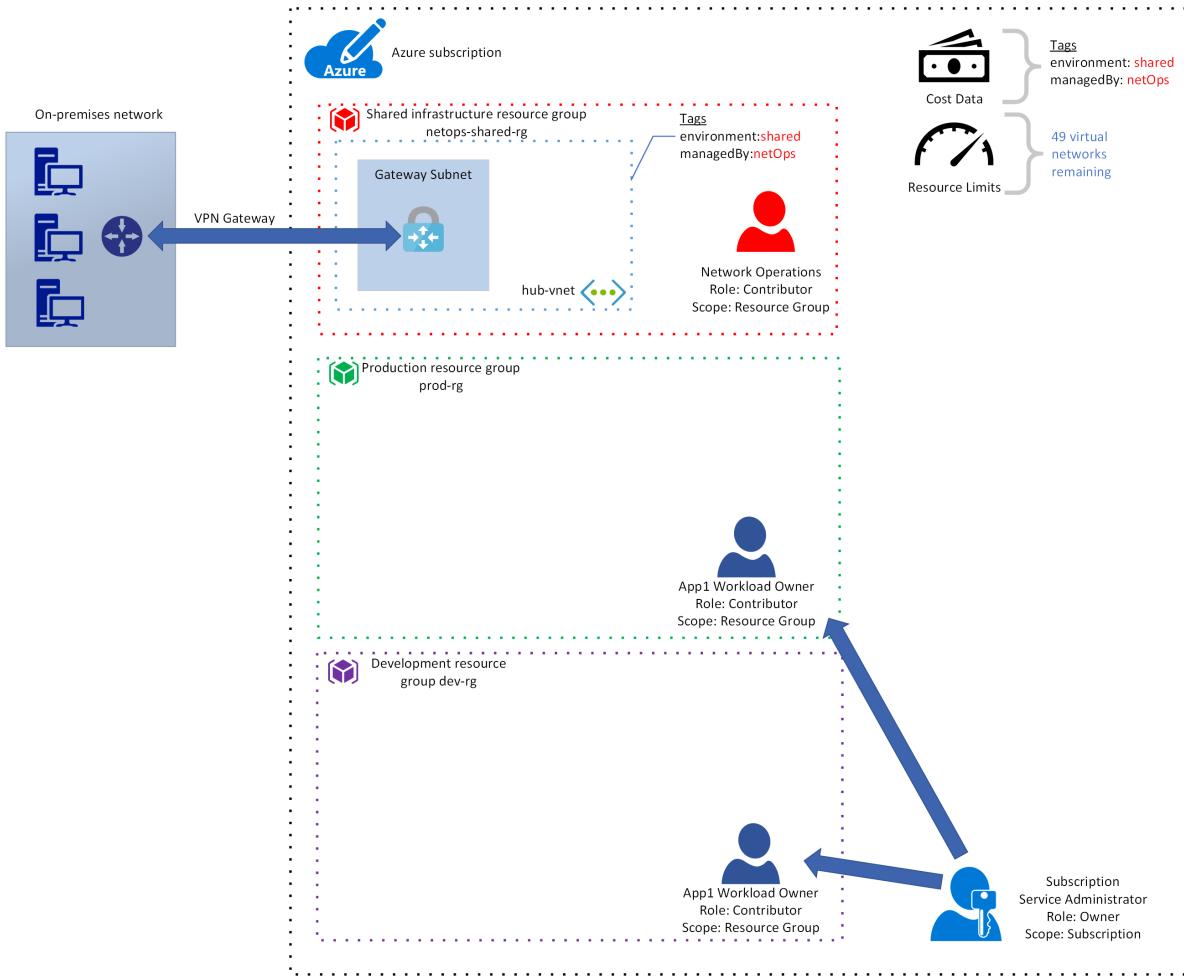
`environment:shared` and `managedBy:netops`. When the **subscription service administrator** exports a cost report, costs will be aligned with each of these tags. This allows the **subscription service administrator** to pivot costs using the `environment` tag and the `managedBy` tag. Notice the **resource limits** counter at the top right-hand side of the figure. Each Azure subscription has **service limits**, and to help you understand the effect of these limits you'll follow the virtual network limit for each subscription. There is a limit of 1,000 virtual networks per subscription, and after the first virtual network is deployed there are now 999 available.



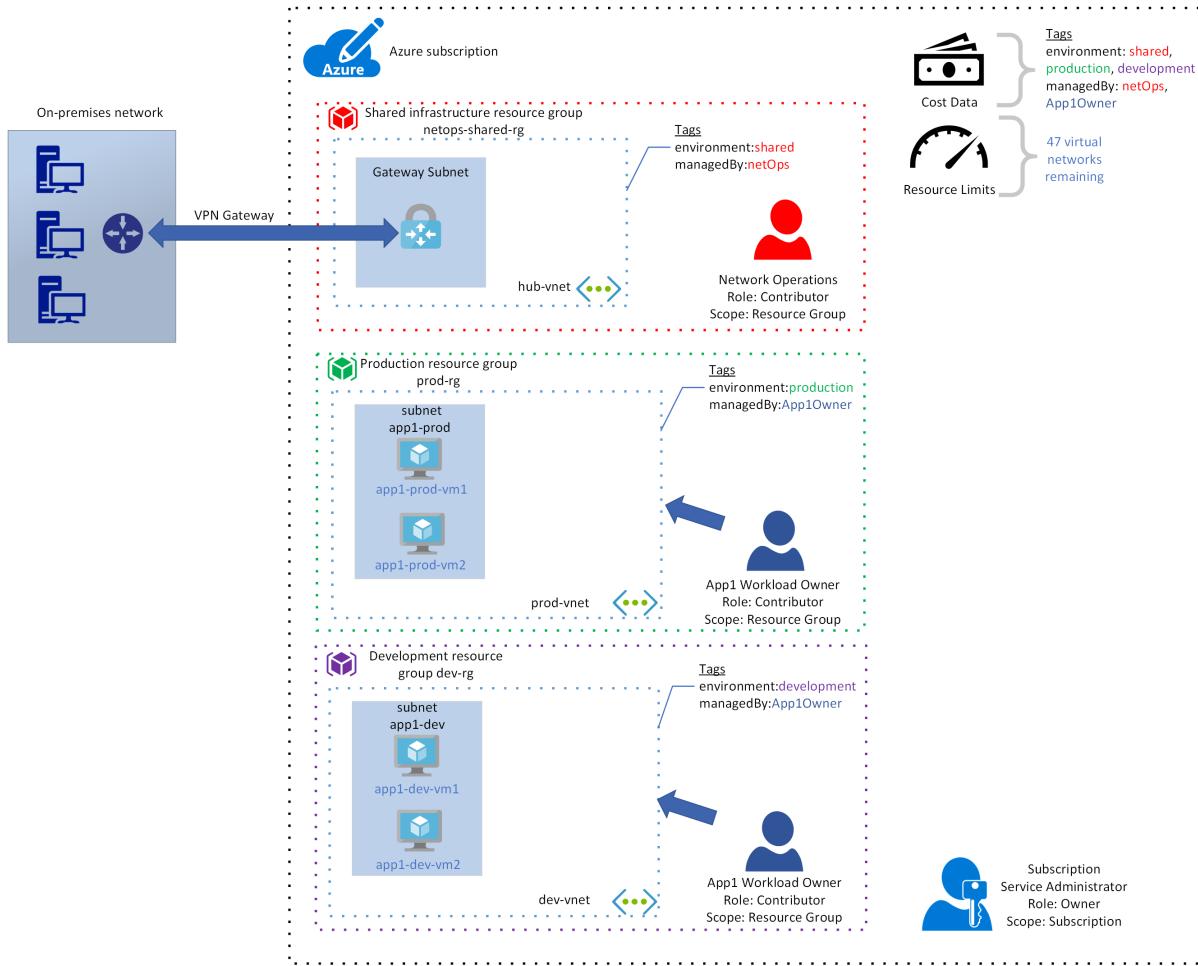
4. Two more resource groups are deployed. The first is named `prod-rg`. This resource group is aligned with the production environment. The second is named `dev-rg` and is aligned with the development environment. All resources associated with production workloads are deployed to the production environment and all resources associated with development workloads are deployed to the development environment. In this example, you'll only deploy two workloads to each of these two environments, so you won't encounter any Azure subscription service limits. Consider that each resource group has a limit of 800 resources per resource group. If you continue to add workloads to each resource group, you'll eventually reach this limit.



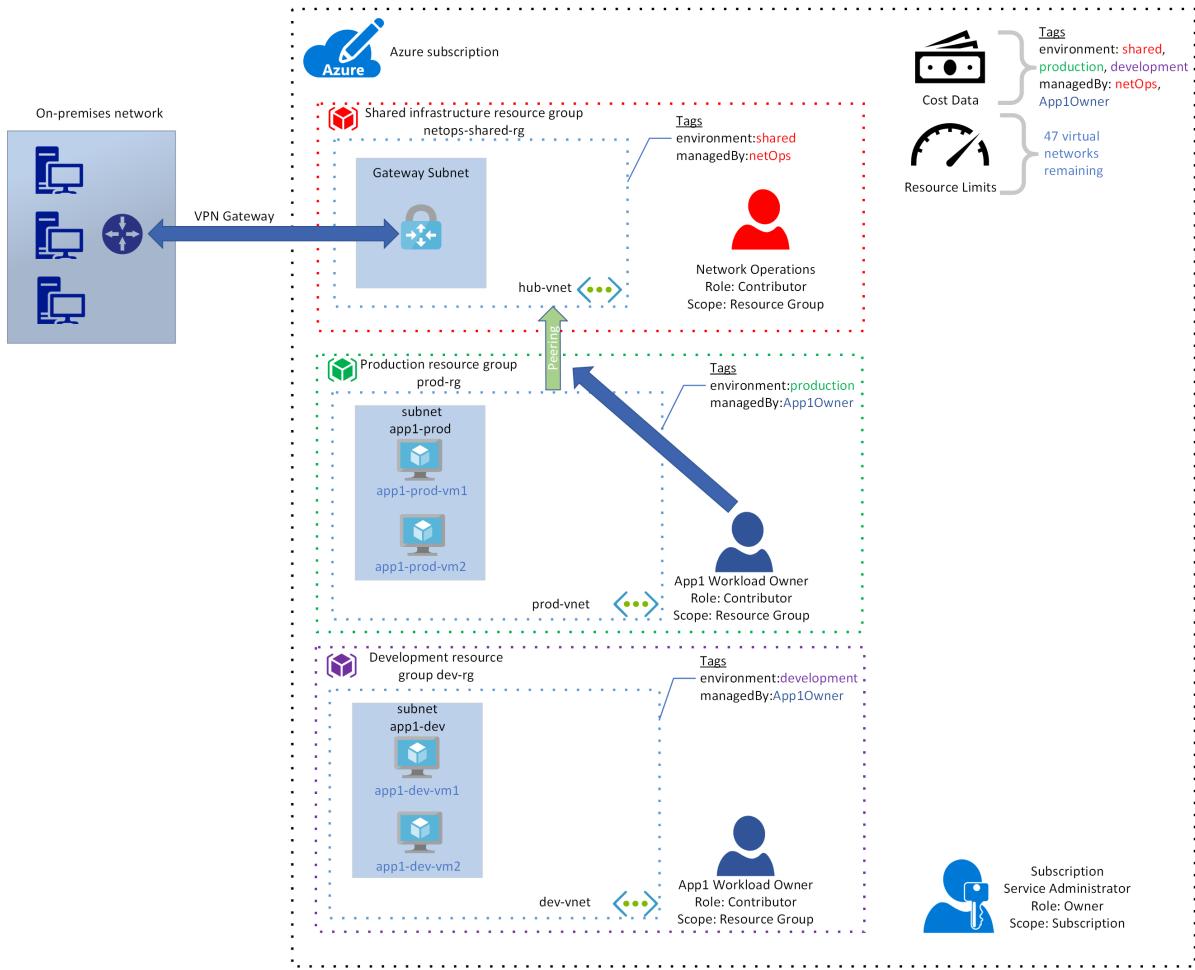
5. The first **workload owner** sends a request to the **subscription service administrator** and is added to each of the development and production environment resource groups with the **contributor** role. As you learned earlier, the **contributor** role allows the user to perform any operation other than assigning a role to another user. The first **workload owner** can now create the resources associated with their workload.



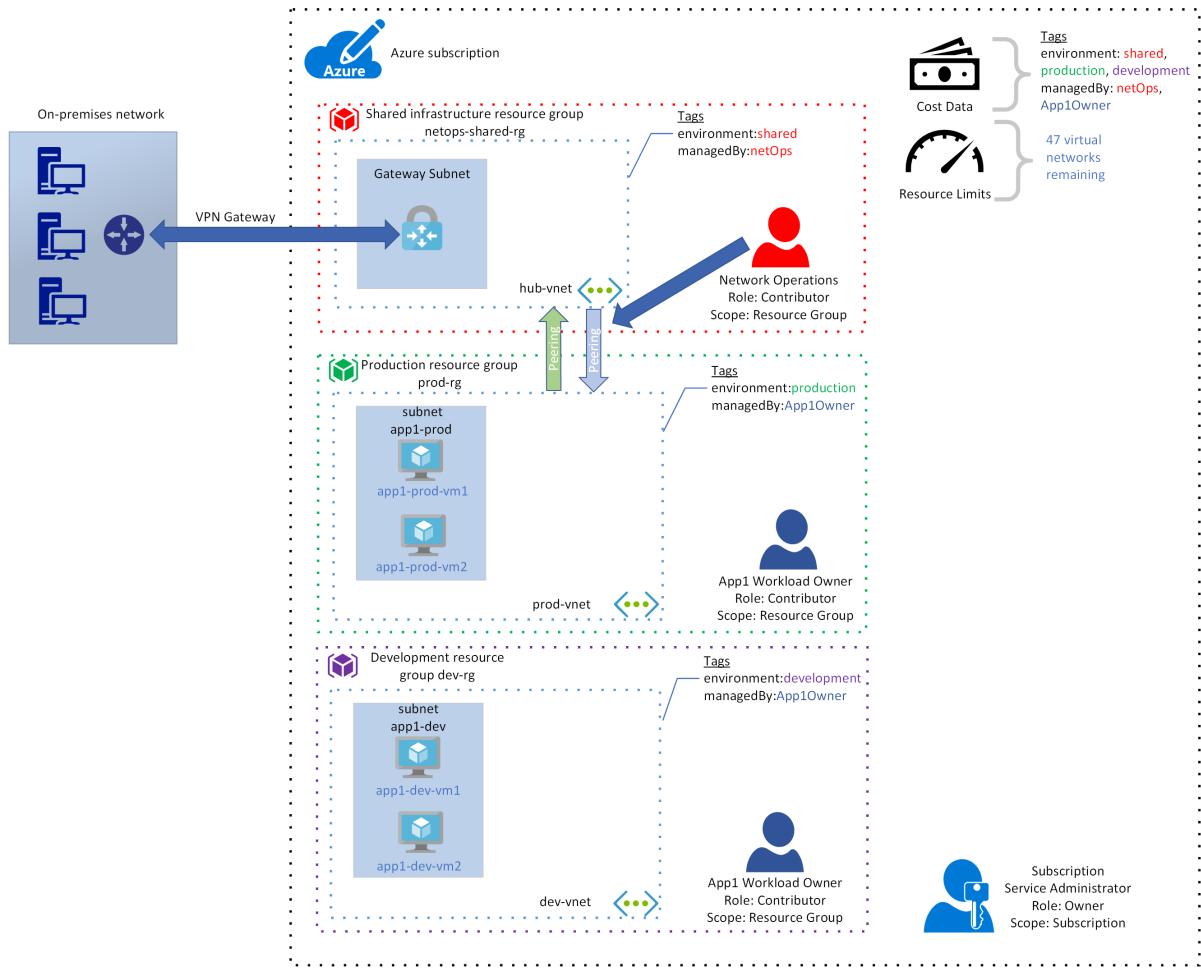
6. The first **workload owner** creates a virtual network in each of the two resource groups with a pair of virtual machines in each. The first **workload owner** applies the `environment` and `managedBy` tags to all resources. Note that the Azure service limit counter is now at 997 virtual networks remaining.



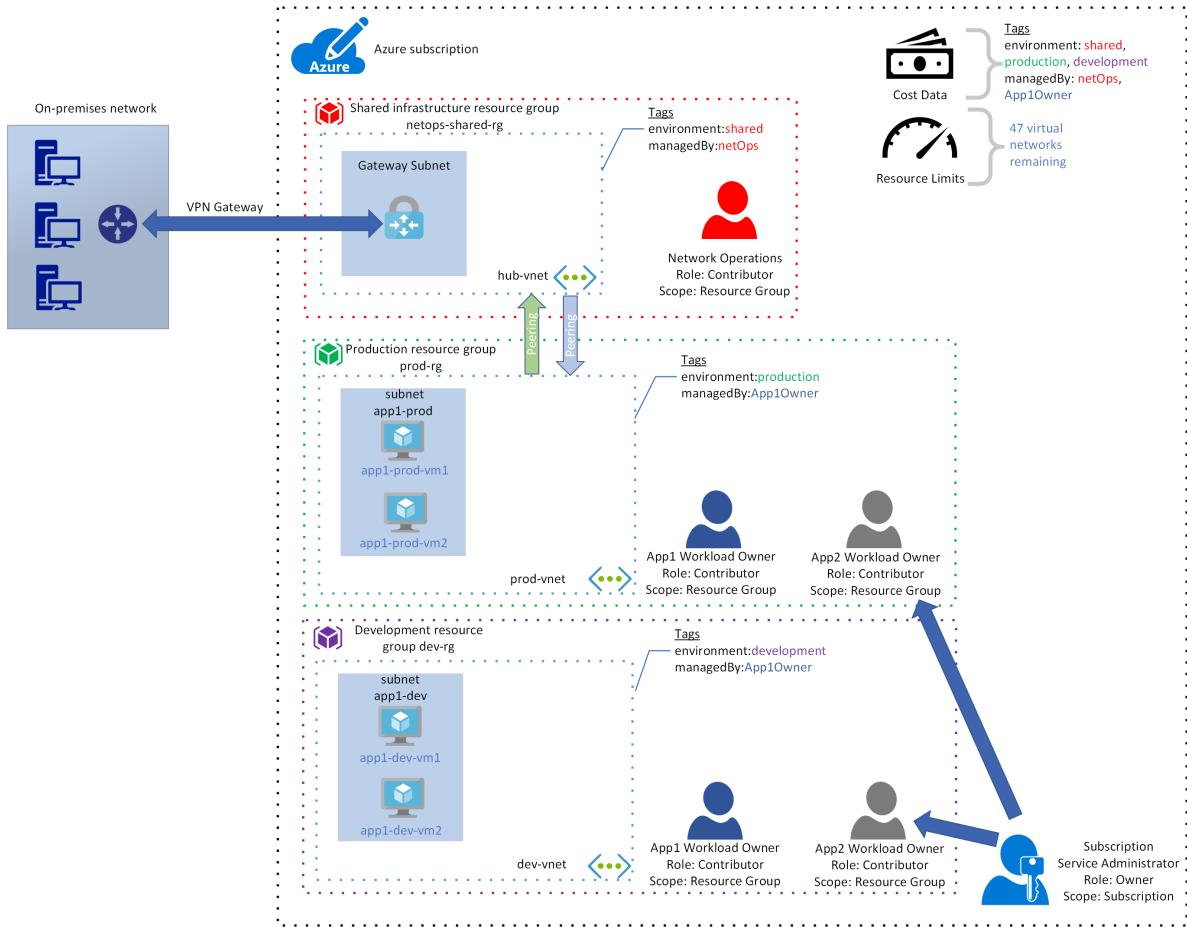
7. None of the virtual networks has connectivity to on-premises when created. In this type of architecture, each virtual network must be peered to the `hub-vnet` in the **shared infrastructure** environment. Virtual network peering creates a connection between two separate virtual networks and allows network traffic to travel between them. Note that virtual network peering is not inherently transitive. A peering must be specified in each of the two virtual networks that are connected, and if only one of the virtual networks specifies a peering, then the connection is incomplete. To illustrate the effect of this, the first **workload owner** specifies a peering between `prod-vnet` and `hub-vnet`. The first peering is created, but no traffic flows because the complementary peering from `hub-vnet` to `prod-vnet` has not yet been specified. The first **workload owner** contacts the **network operations** user and requests this complementary peering connection.



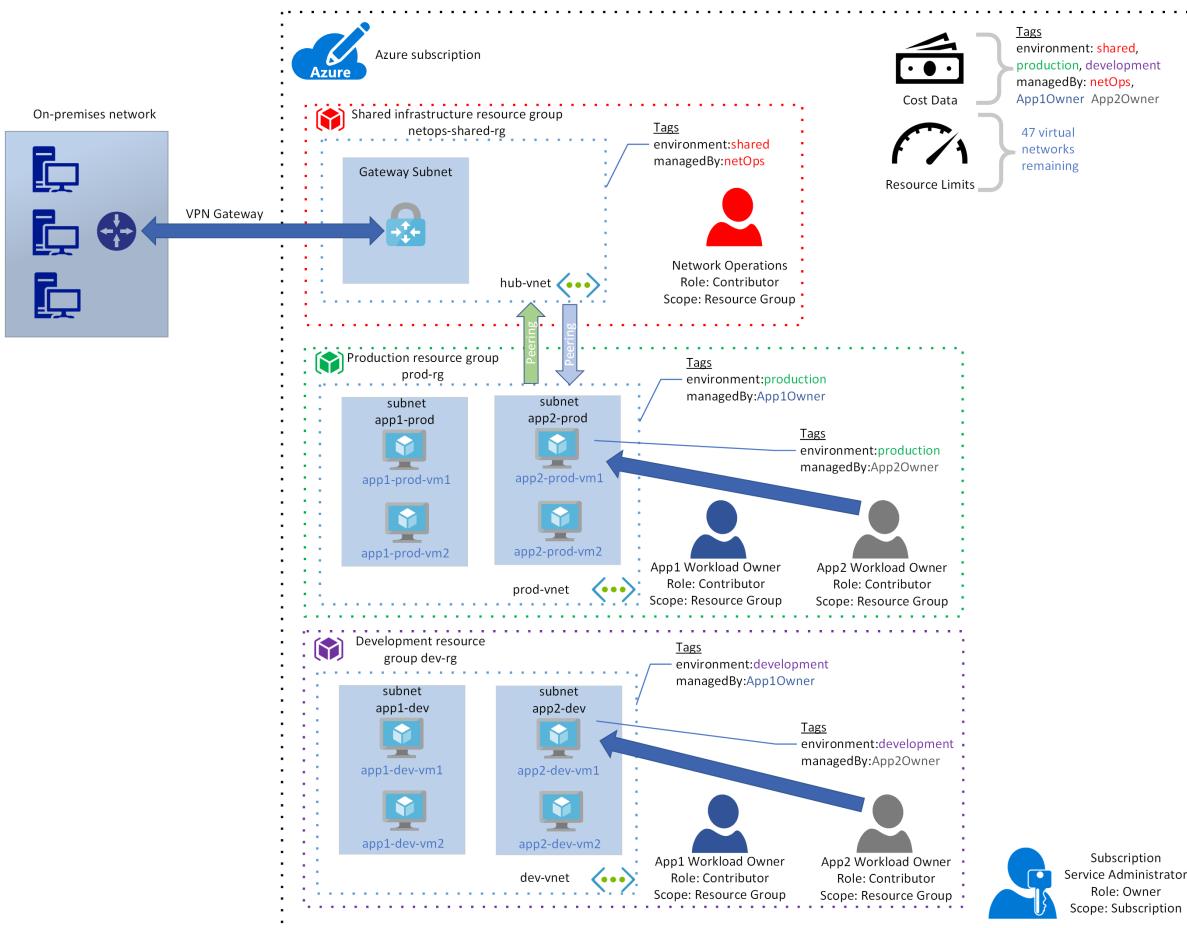
8. The **network operations** user reviews the request, approves it, then specifies the peering in the settings for the **hub-vnet**. The peering connection is now complete, and network traffic flows between the two virtual networks.



- Now, a second **workload owner** sends a request to the **subscription service administrator** and is added to the existing **production** and **development** environment resource groups with the **contributor** role. The second **workload owner** has the same permissions on all resources as the first **workload owner** in each resource group.

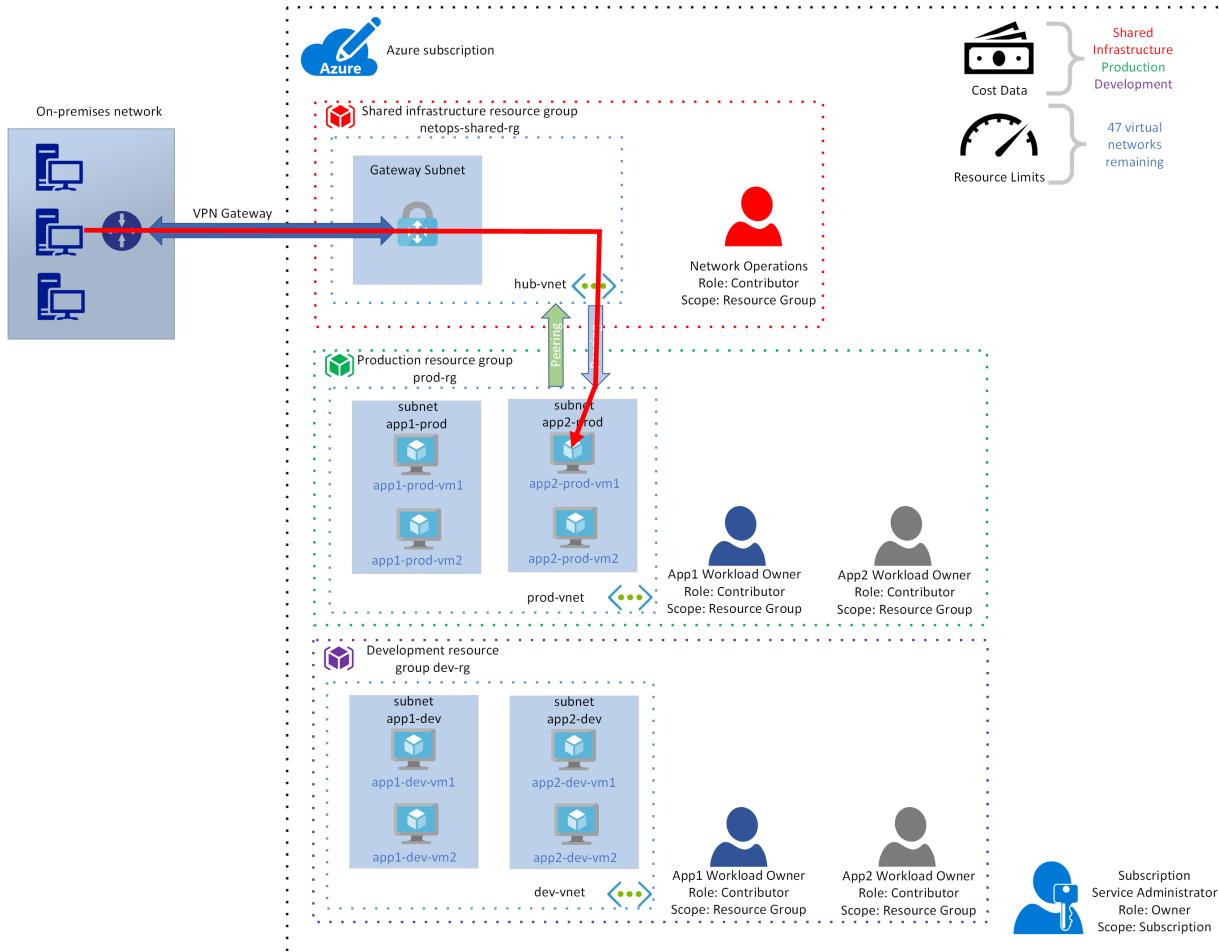


10. The second workload owner creates a subnet in the `prod-vnet` virtual network, then adds two virtual machines. The second workload owner applies the `environment` and `managedBy` tags to each resource.



This example resource management model enables us to manage resources in the three required environments. The shared infrastructure resources are protected because only a single user in the subscription has permission to access those resources. Each of the workload owners can use the shared infrastructure resources without having any permissions on the shared resources themselves. This management model fails the requirement for workload isolation, because both **workload owners** can access the resources of each other's workload.

There's another important consideration with this model that may not be immediately obvious. In the example, it was **app1 workload owner** that requested the network peering connection with the `hub-vnet` to provide connectivity to the on-premises network. The **network operations** user evaluated that request based on the resources deployed with that workload. When the **subscription owner** account added **app2 workload owner** with the **contributor** role, that user had management access rights to all resources in the `prod-rg` resource group.

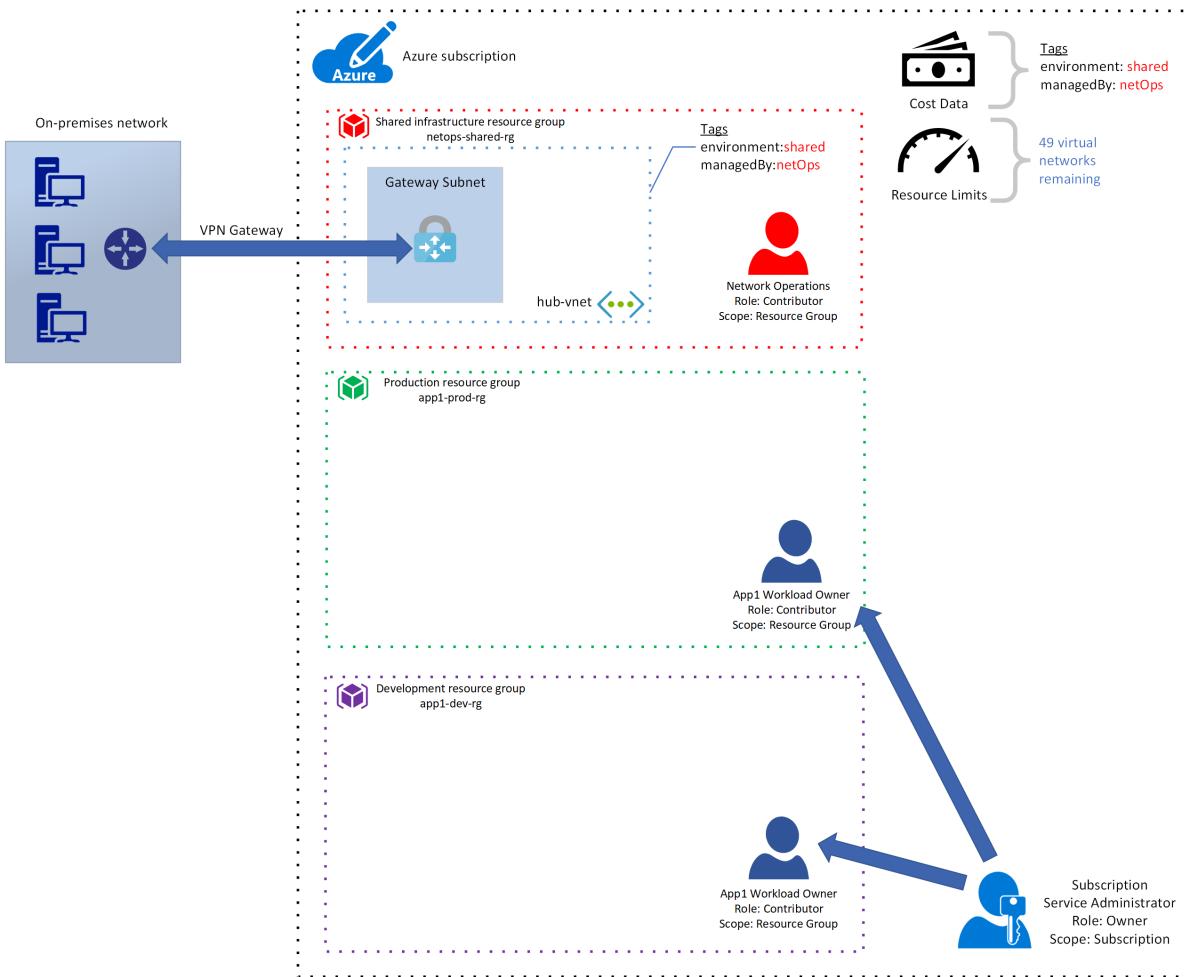


This means **app2 workload owner** had permission to deploy their own subnet with virtual machines in the `prod-vnet` virtual network. By default, those virtual machines have access to the on-premises network. The **network operations** user is not aware of those machines and did not approve their connectivity to on-premises.

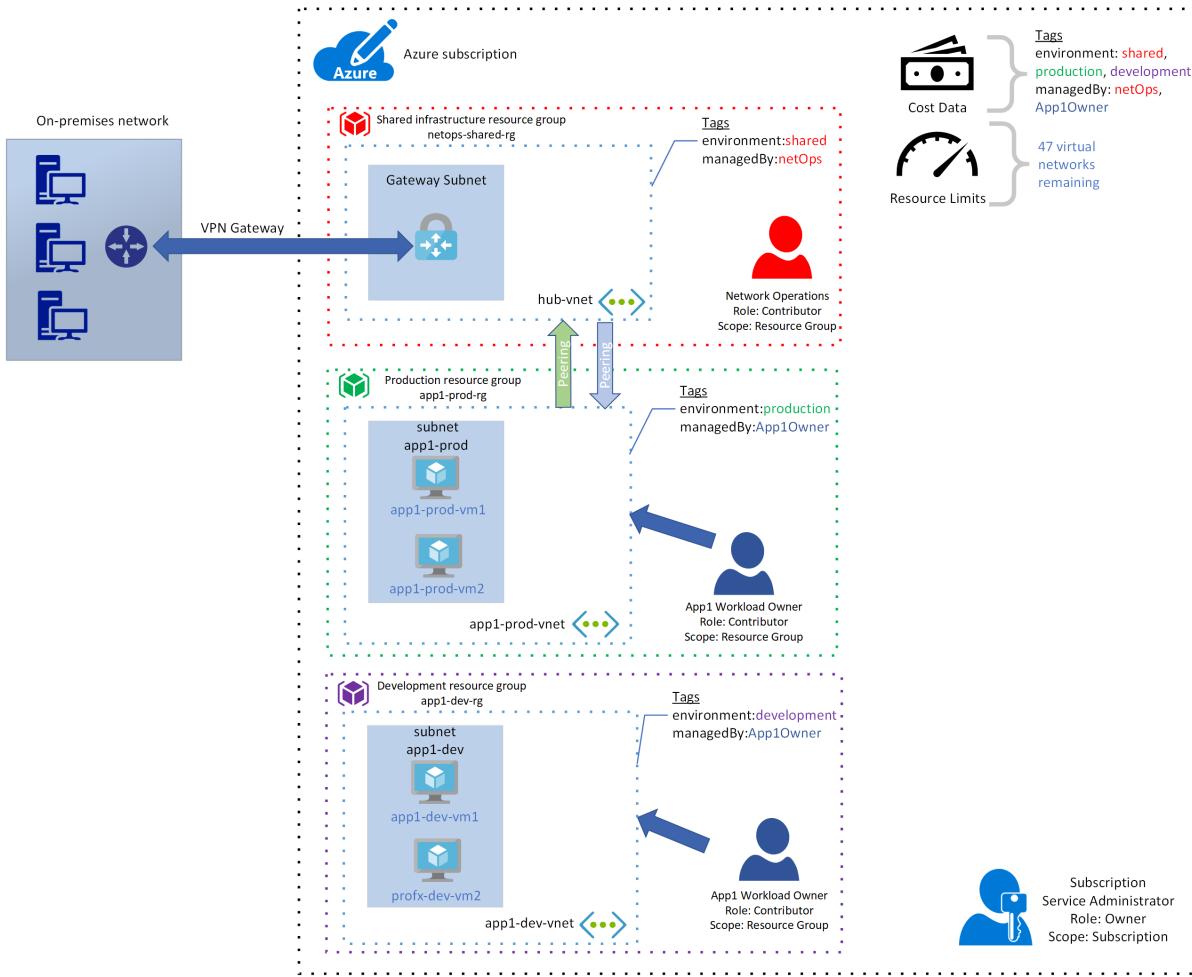
Next, let's look at a single subscription with multiple resource groups for different environments and workloads. Note that in the previous example, the resources for each environment were easily identifiable because they were in the same resource group. Now that you no longer have that grouping, you will have to rely on a resource group naming convention to provide that functionality.

1. The **shared infrastructure** resources will still have a separate resource group in this model, so that remains the same. Each workload requires two resource groups, one for each of the **development** and **production** environments. For the first workload, the **subscription owner** account creates two resource groups. The first is named `app1-prod-rg` and the second is named `app1-dev-rg`. As discussed earlier, this naming convention identifies the resources as being associated with the first workload, `app1`, and either the **development** or **production** environment. Again, the **subscription owner** account adds **app1 workload owner** to the

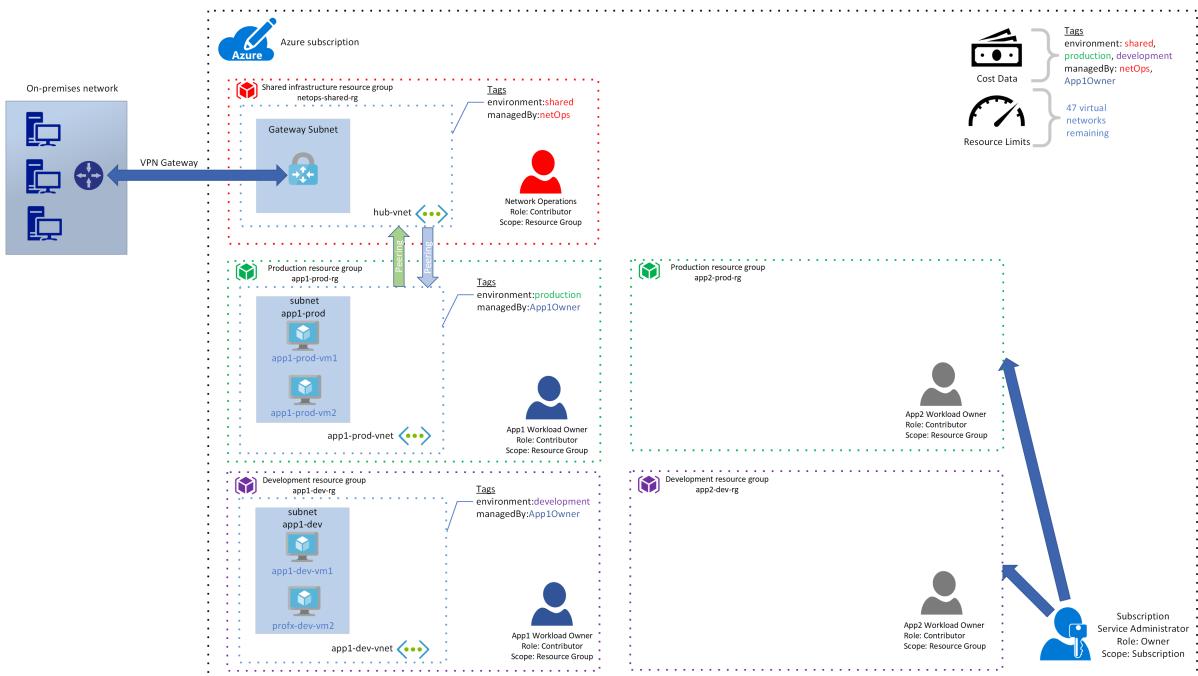
resource group with the **contributor** role.



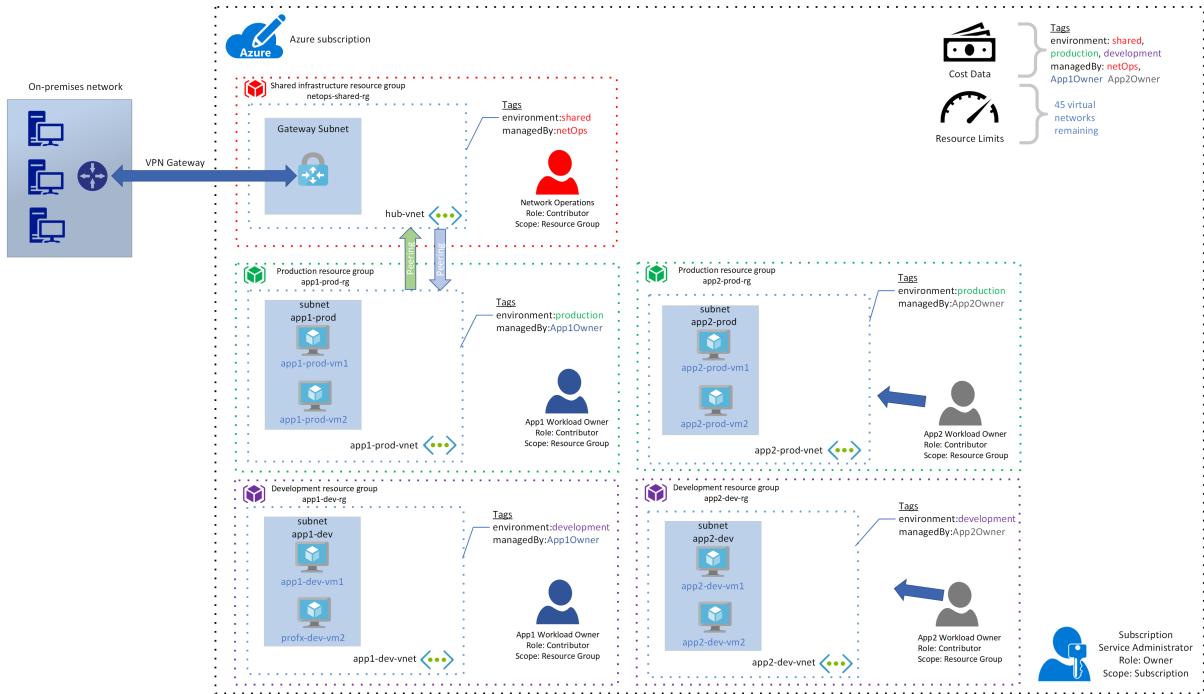
- Similar to the first example, **app1 workload owner** deploys a virtual network named `app1-prod-vnet` to the **production** environment, and another named `app1-dev-vnet` to the **development** environment. Again, **app1 workload owner** sends a request to the **network operations** user to create a peering connection. Note that **app1 workload owner** adds the same tags as in the first example, and the limit counter has been decremented to 997 virtual networks remaining in the subscription.



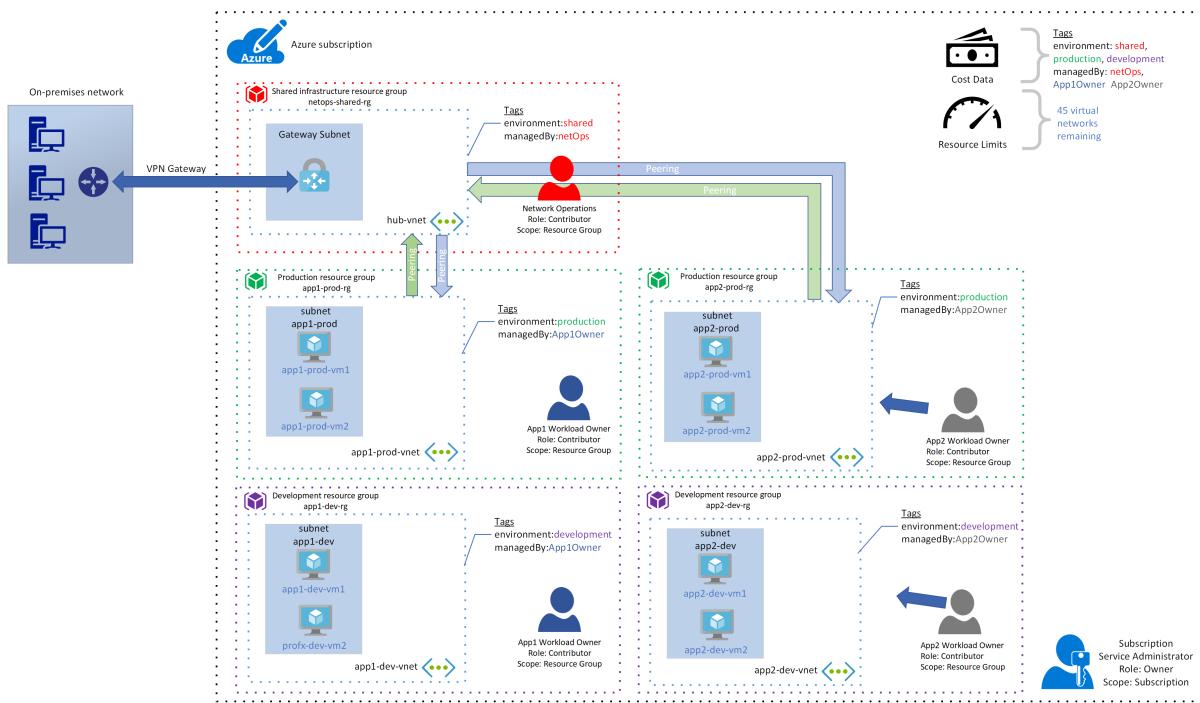
3. The **subscription owner** account now creates two resource groups for **app2 workload owner**. Following the same conventions as for **app1 workload owner**, the resource groups are named **app2-prod-rg** and **app2-dev-rg**. The **subscription owner** account adds **app2 workload owner** to each of the resource groups with the **contributor** role.



4. The **app2 workload owner** account deploys virtual networks and virtual machines to the resource groups with the same naming conventions. Tags are added and the limit counter has been decremented to 995 virtual networks remaining in the subscription.



5. The **app2 workload owner** account sends a request to the **network operations user** to peer the **app2-prod-vnet** with the **hub-vnet**. The **network operations user** creates the peering connection.



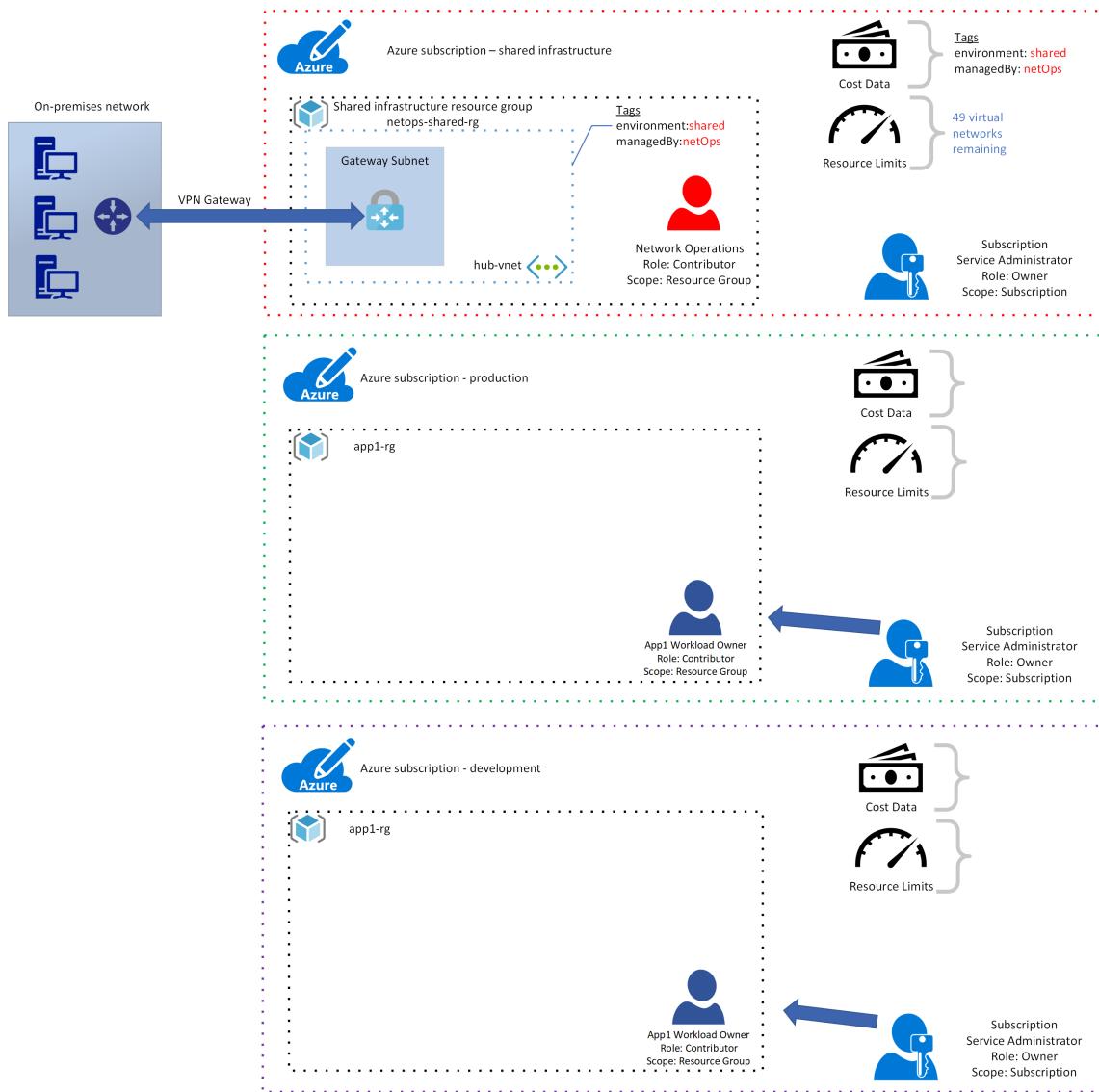
The resulting management model is similar to the first example, with several key differences:

- Each of the two workloads is isolated by workload and by environment.
- This model required two more virtual networks than the first example model. While this is not an important distinction with only two workloads, the theoretical limit on the number of workloads for this model is 24.
- Resources are no longer grouped in a single resource group for each environment. Grouping resources requires an understanding of the naming conventions used for each environment.
- Each of the peered virtual network connections was reviewed and approved by the **network operations user**.

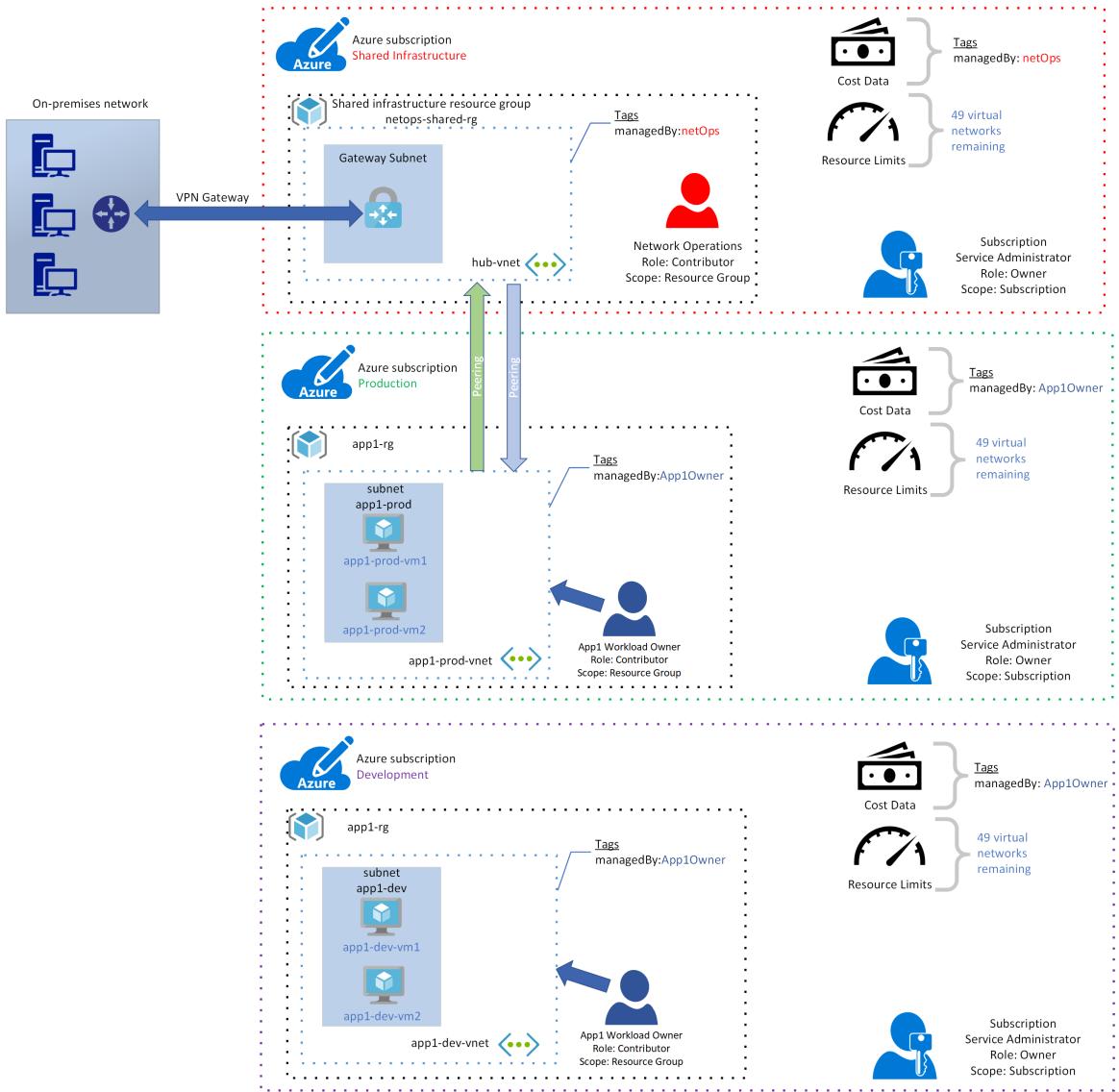
Now let's look at a resource management model using multiple subscriptions. In this model, you'll align each of the three environments to a separate subscription: a **shared services** subscription, **production** subscription, and finally a **development** subscription. The considerations for this model are similar to a model using a single

subscription in that you have to decide how to align resource groups to workloads. Already determined is that creating a resource group for each workload satisfies the workload isolation requirement, so you'll stick with that model in this example.

1. In this model, there are three subscriptions: **shared infrastructure**, **production**, and **development**. Each of these three subscriptions requires a subscription owner, and in the simple example you'll use the same user account for all three. The **shared infrastructure** resources are managed similarly to the first two examples above, and the first workload is associated with the `app1-rg` resource group in the **production** environment and the same-named resource group in the **development** environment. The **app1 workload owner** account is added to each of the resource group with the **contributor** role.



2. As with the earlier examples, **app1 workload owner** creates the resources and requests the peering connection with the **shared infrastructure** virtual network. The **app1 workload owner** account adds only the `managedBy` tag because there is no longer a need for the `environment` tag. That is, resources are for each environment are now grouped in the same **subscription** and the `environment` tag is redundant. The limit counter is decremented to 999 virtual networks remaining.



- Finally, the **subscription owner** account repeats the process for the second workload, adding the resource groups with **app2 workload owner** in the **contributor** role. The limit counter for each of the environment subscriptions is decremented to 998 virtual networks remaining.

This management model has the benefits of the second example above. The key difference is that limits are less of an issue due to the fact that they're spread over two subscriptions. The drawback is that the cost data tracked by tags must be aggregated across all three subscriptions.

Therefore, you can select any of these two examples resource management models depending on the priority of your requirements. If you anticipate that your organization will not reach the service limits for a single subscription, you can use a single subscription with multiple resource groups. Conversely, if your organization anticipates many workloads, multiple subscriptions for each environment may be better.

## Implement the resource management model

You've learned about several different models for governing access to Azure resources. Now you'll walk through the steps necessary to implement the resource management model with one subscription for each of the **shared infrastructure**, **production**, and **development** environments from the design guide. You'll have one **subscription owner** account for all three environments. Each workload will be isolated in a **resource group** with a **workload owner** added with the **contributor** role.

#### **NOTE**

To learn more about the relationship between Azure accounts and subscriptions, see [Understanding resource access in Azure](#).

Follow these steps:

1. Create an [Azure account](#) if your organization doesn't already have one. The person who signs up for the Azure account becomes the Azure account administrator, and your organization's leadership must select an individual to assume this role. This individual will be responsible for:
  - Creating subscriptions.
  - Creating and administering [Azure Active Directory \(Azure AD\)](#) tenants that store user identity for those subscriptions.
2. Your organization's leadership team decides who is responsible for:
  - Management of user identity; an [Azure AD tenant](#) is created by default when your organization's Azure account is created, and the account administrator is added as the [Azure AD global administrator](#) by default. Your organization can choose another user to manage user identity by [assigning the Azure AD global administrator role to that user](#).
  - Subscriptions, which means these users:
    - Manage costs associated with resource usage in that subscription.
    - Implement and maintain least permission model for resource access.
    - Keep track of service limits.
  - Shared infrastructure services (if your organization decides to use this model), which means this user is responsible for:
    - On-premises to Azure network connectivity.
    - Ownership of network connectivity within Azure through virtual network peering.
  - Workload owners.
3. The Azure AD global administrator [creates the new user accounts](#) for:
  - The person who will be the subscription owner for each subscription associated with each environment. Note that this is necessary only if the subscription **service administrator** will not be tasked with managing resource access for each subscription/environment.
  - The person who will be the **network operations user**.
  - The people who are **workload owners**.
4. The Azure account administrator [creates three Azure subscriptions](#):
  - A subscription for the **shared infrastructure** environment.
  - A subscription for the **production** environment.
  - A subscription for the **development** environment.
5. The Azure account administrator [adds the subscription service owner to each subscription](#).
6. Create an approval process for **workload owners** to request the creation of resource groups. The approval process can be implemented in many ways, such as over email, or you can use a process management tool such as [SharePoint workflows](#). The approval process can follow these steps:
  - The **workload owner** prepares a bill of materials for required Azure resources in either the **development** environment, **production** environment, or both, and submits it to the **subscription owner**.
  - The **subscription owner** reviews the bill of materials and validates the requested resources to ensure that the requested resources are appropriate for their planned use, such as checking that the requested [virtual machine sizes](#) are correct.
  - If the request is not approved, the **workload owner** is notified. If the request is approved, the **subscription owner** [creates the requested resource group](#) following your organization's [naming](#)

conventions, adds the **workload owner** with the **contributor role** and sends notification to the **workload owner** that the resource group has been created.

7. Create an approval process for workload owners to request a virtual network peering connection from the shared infrastructure owner. As with the previous step, this approval process can be implemented using email or a process management tool.

Now that you've implemented your governance model, you can deploy your shared infrastructure services.

## Related resources

[Built-in roles for Azure resources](#)

# Deployment Acceleration discipline overview

11/9/2020 • 2 minutes to read • [Edit Online](#)

Deployment acceleration is one of the [Five Disciplines of Cloud Governance](#) within the [Cloud Adoption Framework governance model](#). This discipline focuses on ways of establishing policies to govern asset configuration or deployment. Within the Five Disciplines of Cloud Governance, the Deployment Acceleration discipline includes deployment, configuration alignment, and script reusability. This could be through manual activities or fully automated DevOps activities. In either case, the policies would remain largely the same. As this discipline matures, the cloud governance team can serve as a partner in DevOps and deployment strategies by accelerating deployments and removing barriers to cloud adoption, through the application of reusable assets.

This article outlines the deployment acceleration process that a company experiences during the planning, building, adopting, and operating phases of implementing a cloud solution. It's impossible for any one document to account for all of the requirements of any business. As such, each section of this article outlines suggested minimum and potential activities. The objective of these activities is to help you build a [policy MVP](#), but establish a framework for [incremental policy](#) improvement. The cloud governance team should decide how much to invest in these activities to improve the deployment acceleration position.

## NOTE

The Deployment Acceleration discipline does not replace the existing IT teams, processes, and procedures that allow your organization to effectively deploy and configure cloud-based resources. The primary purpose of this discipline is to identify potential business risks and provide risk-mitigation guidance to the IT staff that are responsible for managing your resources in the cloud. As you develop governance policies and processes make sure to involve relevant IT teams in your planning and review processes.

The primary audience for this guidance is your organization's cloud architects and other members of your cloud governance team. The decisions, policies, and processes that emerge from this discipline should involve engagement and discussions with relevant members of your business and IT teams, especially those leaders responsible for deploying and configuring cloud-based workloads.

## Policy statements

Actionable policy statements and the resulting architecture requirements serve as the foundation of a Deployment Acceleration discipline. Use [sample policy statements](#) as a starting point for defining your Deployment Acceleration policies.

### Caution

The sample policies come from common customer experiences. To better align these policies to specific cloud governance needs, execute the following steps to create policy statements that meet your unique business needs.

## Develop governance policy statements

The following steps help you define governance policies to control deployment and configuration of resources in your cloud environment.

	<p><a href="#">Deployment Acceleration discipline template</a>: Download the template for documenting a Deployment Acceleration discipline.</p>
	<p><a href="#">Business risks</a>: Understand the motives and risks commonly associated with the Deployment Acceleration discipline.</p>
	<p><a href="#">Indicators and metrics</a>: Indicators to understand whether it is the right time to invest in the Deployment Acceleration discipline.</p>
	<p><a href="#">Policy adherence processes</a>: Suggested processes for supporting policy compliance in the Deployment Acceleration discipline.</p>
	<p><a href="#">Maturity</a>: Align cloud management maturity with phases of cloud adoption.</p>
	<p><a href="#">Toolchain</a>: Azure services that can be implemented to support the Deployment Acceleration discipline.</p>

## Next steps

Get started by evaluating [business risks](#) in a specific environment.

[Understand business risks](#)

# Deployment acceleration template

11/9/2020 • 2 minutes to read • [Edit Online](#)

The first step to implementing change is communicating the desired change. The same is true when changing governance practices. The template below serves as a starting point for documenting and communicating policy statements that govern configuration and deployment issues in the cloud. The template also outlines the business criteria that may have led you to create the documented policy statements.

As your discussions progress, use this template's structure as a model for capturing the business risks, risk tolerances, compliance processes, and tooling needed to define your organization's Deployment Acceleration policy statements.

## IMPORTANT

This template is a limited sample. Before updating this template to reflect your requirements, you should review the subsequent steps for defining an effective Deployment Acceleration discipline within your cloud governance strategy.

[Download the Deployment Acceleration discipline template](#)

## Next steps

Solid governance practices start with an understanding of business risk. Review the article on business risks and begin to document the business risks that align with your current cloud adoption plan.

[Understand business risks](#)

# Motivations and business risks in the Deployment Acceleration discipline

11/9/2020 • 2 minutes to read • [Edit Online](#)

This article discusses the reasons that customers typically adopt a Deployment Acceleration discipline within a cloud governance strategy. It also provides a few examples of business risks that drive policy statements.

## Relevance

On-premises systems are often deployed using baseline images or installation scripts. Additional configuration is usually necessary, which may involve multiple steps or human intervention. These manual processes are error-prone and often result in "configuration drift", requiring time-consuming troubleshooting and remediation tasks.

Most Azure resources can be deployed and configured manually via the Azure portal. This approach may be sufficient for your needs when only have a few resources to manage. As your cloud estate grows, your organization should begin to integrate automation into your deployment processes to ensure your cloud resources avoid configuration drift or other problems introduced by manual processes. Adopting a DevOps or [DevSecOps](#) approach is often the best way to manage your deployments as you cloud adoption efforts mature.

A robust deployment acceleration plan ensures that your cloud resources are deployed, updated, and configured correctly and consistently, and remain that way. The maturity of your Deployment Acceleration strategy can also be a significant factor in your [Cost Management strategy](#). Automated provisioning and configuration of your cloud resources allows you to scale down or deallocate resources when demand is low or time-bound, so you only pay for resources as you need them.

## Business risk

The Deployment Acceleration discipline attempts to address the following business risks. During cloud adoption, monitor each of the following for relevance:

- **Service disruption:** Lack of predictable repeatable deployment processes or unmanaged changes to system configurations can disrupt normal operations and can result in lost productivity or lost business.
- **Cost overruns:** Unexpected changes in configuration of system resources can make identifying root cause of issues more difficult, raising the costs of development, operations, and maintenance.
- **Organizational inefficiencies:** Barriers between development, operations, and security teams can cause numerous challenges to effective adoption of cloud technologies and the development of a unified cloud governance model.

## Next steps

Use the [Deployment Acceleration discipline template](#) to document business risks that are likely to be introduced by the current cloud adoption plan.

Once an understanding of realistic business risks is established, the next step is to document the business's tolerance for risk and the indicators and key metrics to monitor that tolerance.

[Metrics, indicators, and risk tolerance](#)

# Risk tolerance metrics and indicators in the Deployment Acceleration discipline

5/21/2020 • 2 minutes to read • [Edit Online](#)

Learn to quantify business risk tolerance associated with the Deployment Acceleration discipline. Defining metrics and indicators helps to create a business case for investing in the maturity of this discipline.

## Metrics

Deployment acceleration focuses on risks related to how cloud resources are configured, deployed, updated, and maintained. The following information is useful when adopting the Deployment Acceleration discipline:

- **Deployment failures:** Percentage of deployments that fail or result in misconfigured resources.
- **Time to deployment:** The amount of time needed to deploy updates to an existing system.
- **Assets out-of-compliance:** The number or percentage of resources that are out of compliance with defined policies.

## Risk tolerance indicators

Risks related to deployment acceleration are largely related to the number and complexity of cloud-based systems deployed for your enterprise. As your cloud estate grows, the number of systems deployed and the frequency of updating your cloud resources will increase. Dependencies between resources magnify the importance of ensuring proper configuration of resources and designing systems for resiliency if one or more resources experiences unexpected downtime.

Traditional corporate IT organizations often have siloed operations, security, and development teams that often do not collaborate well or are even adversarial or hostile toward one another. Recognizing these challenges early and integrating key stakeholders from each of the teams can help ensure agility in your cloud adoption while remaining secure and well-governed. Therefore, consider adopting a DevOps or [DevSecOps](#) organizational culture early in your cloud adoption journey.

Work with your DevSecOps team and business stakeholders to identify [business risks](#) related to configuration, then determine an acceptable baseline for configuration risk tolerance. This section of the Cloud Adoption Framework guidance provides examples, but the detailed risks and baselines for your company or deployments will likely differ.

Once you have a baseline, establish minimum benchmarks representing an unacceptable increase in your identified risks. These benchmarks act as triggers for when you need to take action to remediate these risks. The following are a few examples of how configuration-related metrics, such as those discussed above, can justify an increased investment in the Deployment Acceleration discipline.

- **Configuration drift triggers:** A company that is experiencing unexpected changes in the configuration of key system components, or failures in the deployment of or updates to its systems, should invest in the Deployment Acceleration discipline to identify root causes and steps for remediation.
- **Out of compliance triggers:** If the number of out-of-compliance resources exceeds a defined threshold (either as a total number of resources or a percentage of total resources), a company should invest in Deployment Acceleration discipline improvements to ensure each resource's configuration remains in compliance throughout that resource's lifecycle.
- **Project schedule triggers:** If the time to deploy a company's resources and applications often exceed a define threshold, a company should invest in its deployment acceleration processes to introduce or improve

automated deployments for consistency and predictability. Deployment times measured in days or even weeks usually indicate a suboptimal Deployment Acceleration strategy.

## Next steps

Use the [Deployment Acceleration discipline template](#) to document metrics and tolerance indicators that align to the current cloud adoption plan.

Review sample Deployment Acceleration policies as a starting point to develop your own policies to address specific business risks aligned with your cloud adoption plans.

[Review sample policies](#)

# Deployment Acceleration sample policy statements

11/9/2020 • 3 minutes to read • [Edit Online](#)

Individual cloud policy statements are guidelines for addressing specific risks identified during your risk assessment process. These statements should provide a concise summary of risks and plans to deal with them. Each statement definition should include these pieces of information:

- **Technical risk:** A summary of the risk this policy will address.
- **Policy statement:** A clear summary explanation of the policy requirements.
- **Design options:** Actionable recommendations, specifications, or other guidance that IT teams and developers can use when implementing the policy.

The following sample policy statements address common configuration-related business risks. These statements are examples you can reference when drafting policy statements to address your organization's needs. These examples are not meant to be prescriptive, and there are potentially several policy options for dealing with each identified risk. Work closely with business and IT teams to identify the best policies for your unique set of risks.

## Reliance on manual deployment or configuration of systems

**Technical risk:** Relying on human intervention during deployment or configuration increases the likelihood of human error and reduces the repeatability and predictability of system deployments and configuration. It also typically leads to slower deployment of system resources.

**Policy statement:** All assets deployed to the cloud should be deployed using templates or automation scripts whenever possible.

**Potential design options:** [Azure Resource Manager templates](#) enable using infrastructure as code to deploy your resources to Azure. You could also use [Terraform](#) as a consistent on-premises and cloud-based deployment tool.

## Lack of visibility into system issues

**Technical risk:** Insufficient monitoring and diagnostics for business systems prevent operations personnel from identifying and remediating issues before a system outage occurs, and can significantly increase the time needed to properly resolve an outage.

**Policy statement:** The following policies will be implemented:

- Key metrics and diagnostics measures will be identified for all production systems and components, and monitoring and diagnostic tools will be applied to these systems and monitored regularly by operations personnel.
- Operations will consider using monitoring and diagnostic tools in nonproduction environments such as staging and QA to identify system issues before they occur in the production environment.

**Potential design options:** [Azure Monitor](#), including Log Analytics and Application Insights, provides tools for collecting and analyzing telemetry to help you understand how your applications are performing and proactively identify issues affecting them and the resources they depend on. Additionally, [Azure activity log](#) reports all changes that are being made at the platform level and should be monitored and audited for noncompliant changes.

## Configuration security reviews

**Technical risk:** Over time, new security threats or concerns can increase the risks of unauthorized access to

secure resources.

**Policy statement:** Cloud governance processes must include monthly review with configuration management teams to identify malicious actors or usage patterns that should be prevented by cloud asset configuration.

**Potential design options:** Establish a monthly security review meeting that includes both governance team members and IT staff responsible for configuration cloud applications and resources. Review existing security data and metrics to establish gaps in current Deployment Acceleration policy and tooling, and update policy to remediate any new risks.

## Next steps

Use the samples mentioned in this article as a starting point to develop policies that address specific business risks that align with your cloud adoption plans.

To begin developing your own custom Identity Baseline policy statements, download the [Identity Baseline discipline template](#).

To accelerate adoption of this discipline, choose the [actionable governance guide](#) that most closely aligns with your environment. Then modify the design to incorporate your specific corporate policy decisions.

Building on risks and tolerance, establish a process for governing and communicating Deployment Acceleration policy adherence.

[Establish policy compliance processes](#)

# Deployment Acceleration policy compliance processes

11/9/2020 • 4 minutes to read • [Edit Online](#)

This article discusses an approach to policy-adherence processes that govern the [Deployment Acceleration discipline](#). Effective governance of cloud configuration starts with recurring manual processes designed to detect issues and impose policies to remediate those risks. You can automate these processes and supplement to reduce the overhead of governance and allow for faster response to deviation.

## Planning, review, and reporting processes

The best Deployment Acceleration tools in the cloud are only as good as the processes and policies that they support. The following is a set of example processes commonly used as part of a Deployment Acceleration discipline. Use these examples as a starting point when planning the processes that will allow you to continue to update deployment and configuration policy based on business change and feedback from the development and IT teams responsible for turning governance guidance into action.

**Initial risk assessment and planning:** As part of your initial adoption of the Deployment Acceleration discipline, identify your core business risks and tolerances related to deployment of your business applications. Use this information to discuss specific technical risks with members of the IT operations team, and develop a baseline set of deployment and configuration policies for remediating these risks to establish your initial governance strategy.

**Deployment planning:** Before deploying any asset, perform a security and operations review to identify any new risks and ensure all deployment related policy requirements are met.

**Deployment testing:** As part of the deployment process for any asset, the cloud governance team, in cooperation with your IT operations teams, is responsible for reviewing the deployment policy compliance.

**Annual planning:** Conduct an annual high-level review of Deployment Acceleration strategy. Explore future corporate priorities and updated cloud adoption strategies to identify potential risk increase and other emerging configuration needs and opportunities. Also use this time to review the latest DevOps best practices and integrate these into your policies and review processes.

**Quarterly review and planning:** Conduct a quarterly review of operational audit data and incident reports to identify any changes required in Deployment Acceleration policy. As part of this process, review current DevOps and devtechops best practices, and update policy as appropriate. After the review is complete, align application and systems design guidance with updated policy.

This planning process is also a good time to evaluate the current membership of your cloud governance team for knowledge gaps related to new or changing policy and risks related to DevOps and deployment acceleration. Invite relevant IT staff to participate in reviews and planning as either temporary technical advisors or permanent members of your team.

**Education and training:** On a bimonthly basis, offer training sessions to make sure IT staff and developers are up-to-date on the latest Deployment Acceleration strategy and requirements. As part of this process review and update any documentation, guidance, or other training assets to ensure they're in sync with the latest corporate policy statements.

**Monthly audit and reporting reviews:** Perform a monthly audit on all cloud deployments to assure their continued alignment with configuration policy. Review deployment-related activities with IT staff and identify any

compliance issues not already handled as part of the ongoing monitoring and enforcement process. The result of this review is a report for the cloud strategy team and each cloud adoption team to communicate overall adherence to policy. The report is also stored for auditing and legal purposes.

## Processes for ongoing monitoring

A successful Deployment Acceleration strategy depends on visibility into the current and past state of your cloud infrastructure. Without the ability to analyze the relevant metrics and data of your cloud resources operational health and activity, you cannot identify changes in your risks or detect violations of your risk tolerances. The ongoing governance processes discussed above require quality data to ensure policy can be modified to protect your infrastructure against changing threats and risks from misconfigured resources.

Ensure that your IT operations teams have implemented automated monitoring systems for your cloud infrastructure that capture the relevant logs data you need to evaluate risk. Be proactive in monitoring these systems to ensure prompt detection and mitigation of potential policy violation, and ensure your monitoring strategy is in line with deployment and configuration needs.

## Violation triggers and enforcement actions

Because noncompliance with configuration policies can lead to critical service disruption risks, the cloud governance team should have visibility into serious policy violations. Ensure IT staff have clear escalation paths for reporting configuration compliance issues to the governance team members best suited to identify and verify that policy issues are mitigated when detected.

When violations are detected, you should take actions to realign with policy as soon as possible. Your IT team can automate most violation triggers using the tools outlined in the [Deployment Acceleration toolchain for Azure](#).

The following triggers and enforcement actions provide examples you can use when discussing how to use monitoring data to resolve policy violations:

- **Unexpected changes in configuration detected.** If the configuration of a resource changes unexpectedly, work with IT staff and workload owners to identify root cause and develop a remediation plan.
- **Configuration of new resources does not adhere to policy.** Work with DevOps teams and workload owners to review Deployment Acceleration policies during project startup so everyone involved understands the relevant policy requirements.
- **Deployment failures or configuration issues cause delays in project schedules.** Work with development teams and workload owners to ensure the team understands how to automate the deployment of cloud-based resources for consistency and repeatability. Fully automated deployments should be required early in the development cycle. Trying to accomplish this later usually leads to unexpected issues and delays.

## Next steps

Use the [Deployment Acceleration discipline template](#) to document the processes and triggers that align to the current cloud adoption plan.

For guidance on executing cloud management policies in alignment with adoption plans, see [Deployment Acceleration discipline improvement](#).

[Deployment Acceleration discipline improvement](#)

# Deployment Acceleration discipline improvement

11/9/2020 • 4 minutes to read • [Edit Online](#)

The Deployment Acceleration discipline focuses on establishing policies that ensure that resources are deployed and configured consistently and repeatably, and remain in compliance throughout their lifecycle. Within the Five Disciplines of Cloud Governance, the Deployment Acceleration discipline includes decisions regarding automating deployments, source-controlling deployment artifacts, monitoring deployed resources to maintain desired state, and auditing any compliance issues.

This article outlines some potential tasks your company can engage in to better develop and mature the Deployment Acceleration discipline. These tasks can be broken down into planning, building, adopting, and operating phases of implementing a cloud solution, which are then iterated on allowing the development of an [incremental approach to cloud governance](#).

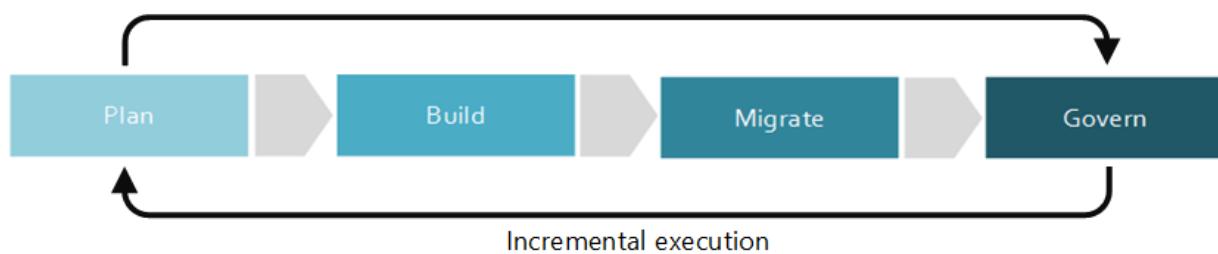


Figure 1: Phases of an incremental approach to cloud governance.

It's impossible for any one document to account for the requirements of all businesses. As such, this article outlines suggested minimum and potential example activities for each phase of the governance maturation process. The initial objective of these activities is to help you build a [policy MVP](#) and establish a framework for incremental policy improvement. Your cloud governance team will need to decide how much to invest in these activities to improve your Identity Baseline discipline.

#### Caution

Neither the minimum or potential activities outlined in this article are aligned to specific corporate policies or third-party compliance requirements. This guidance is designed to help facilitate the conversations that will lead to alignment of both requirements with a cloud governance model.

## Planning and readiness

This phase of governance maturity bridges the divide between business outcomes and actionable strategies. During this process, the leadership team defines specific metrics, maps those metrics to the digital estate, and begins planning the overall migration effort.

#### Minimum suggested activities:

- Evaluate your [Deployment Acceleration toolchain](#) options and implement a hybrid strategy that is appropriate to your organization.
- Develop a draft architecture guidelines document and distribute to key stakeholders.
- Educate and involve the people and teams affected by the development of architecture guidelines.
- Train development teams and IT staff to understand DevSecOps principles and strategies and the importance of fully automated deployments in the Deployment Acceleration discipline.

#### Potential activities:

- Define roles and assignments that will govern deployment acceleration in the cloud.

## Build and predeployment

### Minimum suggested activities:

- For new cloud-based applications, introduce fully automated deployments early in the development process. This investment will improve the reliability of your testing processes and ensure consistency across your development, QA, and production environments.
- Store all deployment artifacts such as deployment templates or configuration scripts using a source-control platform such as GitHub or Azure DevOps.
- Store all secrets, passwords, certificates, and connection strings in [Azure Key Vault](#).
- Consider a pilot test before implementing your [Deployment Acceleration toolchain](#), making sure it streamlines your deployments as much as possible. Apply feedback from pilot tests during the predeployment phase, repeating as needed.
- Evaluate the logical and physical architecture of your applications, and identify opportunities to automate the deployment of application resources or improve portions of the architecture using other cloud-based resources.
- Update the architecture guidelines document to include deployment and user adoption plans, and distribute to key stakeholders.
- Continue to educate the people and teams most affected by the architecture guidelines.

### Potential activities:

- Define a continuous integration and continuous deployment (CI/CD) pipeline to fully manage releasing updates to your application through your development, QA, and production environments.

## Adopt and migrate

Migration is an incremental process that focuses on the movement, testing, and adoption of applications or workloads in an existing digital estate.

### Minimum suggested activities:

- Migrate your [Deployment Acceleration toolchain](#) from development to production.
- Update the architecture guidelines document and distribute to key stakeholders.
- Develop educational materials and documentation, awareness communications, incentives, and other programs to help drive developer and IT adoption.

### Potential activities:

- Validate that the best practices defined during the build and predeployment phases are properly executed.
- Ensure that each application or workload aligns with the Deployment Acceleration strategy before release.

## Operate and post-implementation

Once the transformation is complete, governance and operations must live on for the natural lifecycle of an application or workload. This phase of governance maturity focuses on the activities that commonly come after the solution is implemented and the transformation cycle begins to stabilize.

### Minimum suggested activities:

- Customize your [Deployment Acceleration toolchain](#) based on your organization's changing needs.
- Automate notifications and reports to alert you of potential configuration issues or malicious threats.
- Monitor and report on application and resource usage.

- Report on post-deployment metrics and distribute to stakeholders.
- Revise the architecture guidelines to guide future adoption processes.
- Continue to communicate with and train the affected people and teams on a regular basis to ensure ongoing adherence to architecture guidelines.

#### Potential activities:

- Configure a desired state configuration monitoring and reporting tool.
- Regularly review configuration tools and scripts to improve processes and identify common issues.
- Work with development, operations, and security teams to help mature DevSecOps practices and break down organizational silos that lead to inefficiencies.

## Next steps

Now that you understand the concept of cloud identity governance, examine the [Identity Baseline toolchain](#) to identify Azure tools and features that you'll need when developing your Identity Baseline discipline on the Azure platform.

[Identity Baseline toolchain for Azure](#)

# Deployment Acceleration tools in Azure

11/9/2020 • 2 minutes to read • [Edit Online](#)

The [Deployment Acceleration discipline](#) is one of the [Five Disciplines of Cloud Governance](#). This discipline focuses on ways of establishing policies to govern asset configuration or deployment. Within the Five Disciplines of Cloud Governance, the Deployment Acceleration discipline involves deployment and configuration alignment. This could be through manual activities or fully automated DevOps activities. In either case, the policies involved would remain largely the same.

Cloud custodians, cloud guardians, and cloud architects with an interest in governance are each likely to invest a lot of time in the Deployment Acceleration discipline, which codifies policies and requirements across multiple cloud adoption efforts. The tools in this toolchain are important to the cloud governance team and should be a high priority on the learning path for the team.

The following is a list of Azure tools that can help mature the policies and processes that support this discipline.

	AZURE POLICY	AZURE MANAGEMENT GROUPS	AZURE RESOURCE MANAGER	AZURE BLUEPRINTS	AZURE RESOURCE GRAPH	AZURE COST MANAGEMENT + BILLING
Implement corporate policies	Yes	No	No	No	No	No
Apply policies across subscriptions	Required	Yes	No	No	No	No
Deploy defined resources	No	No	Yes	No	No	No
Create fully compliant environments	Required	Required	Required	Yes	No	No
Audit policies	Yes	No	No	No	No	No
Query Azure resources	No	No	No	No	Yes	No
Report on cost of resources	No	No	No	No	No	Yes

The following are additional tools that may be required to accomplish specific deployment acceleration objectives. Often these tools are used outside of the governance team, but are still considered an aspect of the Deployment Acceleration discipline.

	AZURE PORTAL	AZURE RESOURCE MANAGER	AZURE POLICY	AZURE DEVOPS	AZURE BACKUP	AZURE SITE RECOVERY
Manual deployment (single asset)	Yes	Yes	No	Not efficiently	No	Yes
Manual deployment (full environment)	Not efficiently	Yes	No	Not efficiently	No	Yes
Automated deployment (full environment)	No	Yes	No	Yes	No	Yes
Update configuration of a single asset	Yes	Yes	Not efficiently	Not efficiently	No	Yes, during replication
Update configuration of a full environment	Not efficiently	Yes	Yes	Yes	No	Yes, during replication
Manage configuration drift	Not efficiently	Not efficiently	Yes	Yes	No	Yes, during replication
Create an automated pipeline to deploy code and configure assets (DevOps)	No	No	No	Yes	No	No

Aside from the Azure native tools mentioned above, it is common for customers to use third-party tools to facilitate deployment acceleration and DevOps deployments.

# Cloud management in the Cloud Adoption Framework

11/9/2020 • 2 minutes to read • [Edit Online](#)

Delivering on a [cloud strategy](#) requires solid planning, readiness, and adoption. But it's the ongoing operation of the digital assets that delivers tangible business outcomes. Without a plan for reliable, well-managed operations of the cloud solutions, those efforts will yield little value. The following exercises help develop the business and technical approaches needed to provide cloud management that powers ongoing operations.

## Get started

To prepare you for this phase of the cloud adoption lifecycle, the framework suggests the following exercises:

1	<p><b>Establish a management baseline:</b> Define the criticality classifications, cloud management tools, and processes required to deliver your minimum commitment to operations management.</p>
2	<p><b>Define business commitments:</b> Document supported workloads to establish operational commitments with the business and agree on cloud management investments for each workload.</p>
3	<p><b>Expand the management baseline:</b> Based on business commitments and operations decisions, make use of the included best practices to implement the required cloud management tooling.</p>
4	<p><b>Advanced operations and design principles:</b> Platforms or workloads that require a higher level of business commitment might require a deeper architecture review to deliver on resiliency and reliability commitments.</p>

The preceding steps create actionable approaches to deliver on the Cloud Adoption Framework's Manage methodology.

## Manage

## Business alignment

### Criticality



Document the criticality and relative business value of each workload.

### Impact



Establish clear performance expectations and business interruption time/value metrics.

### Commitment



Document, track, and report on commitments to cost and performance

## Cloud Operations Disciplines



### Inventory and visibility

Establish a defined inventory of assets. Develop visibility into the asset telemetry.



### Operational compliance

Manage configuration drift and standards. Apply management automation and controls.



### Protect and recover

Implement solutions to minimize performance interruptions and ensure rapid recovery, when needed.



### Platform operations

Customize operations to improve performance of the common platforms that support multiple workloads.



### Workload operations

Understand workload telemetry and align workload operations to performance and reliability commitments.

As discussed in the [business alignment](#) article, not all workloads are mission critical. Within any portfolio are various degrees of operational management needs. Business alignment efforts aid in capturing the business impact and negotiating management costs with the business, to ensure the most appropriate operational management processes and tools.

The guidance in the manage section of the Cloud Adoption Framework serves two purposes:

- Provides examples of actionable operations management approaches that represent common experiences often encountered by customers.
- Helps you create personalized management solutions based on business commitments.

This content is intended for use by the cloud operations team. It's also relevant to cloud architects who need to develop a strong foundation in cloud operations or cloud design principles.

The content in the Cloud Adoption Framework affects the business, technology, and culture of enterprises. This section of the Cloud Adoption Framework interacts heavily with IT operations, IT governance, finance, line-of-business leaders, networking, identity, and cloud adoption teams. Various dependencies on these personnel require a facilitative approach by the cloud architects who are using this guidance. Facilitation with these teams is seldom a one-time effort.

The cloud architect serves as the thought leader and facilitator to bring these audiences together. The content in this collection of guides is designed to help the cloud architect facilitate the right conversation, with the right audience, to drive necessary decisions. Business transformation that's empowered by the cloud depends on the cloud architect to help guide decisions throughout the business and IT.

Each section of the Cloud Adoption Framework represents a different specialization or variant of the cloud architect role. This section of the Cloud Adoption Framework is designed for cloud architects with a passion for operations and management of deployment solutions. Within this framework, these specialists are referred to frequently as *cloud operations*, or collectively as the *cloud operations team*.

If you want to follow this guide from beginning to end, this content aids in developing a robust cloud operations strategy. The guidance walks you through the theory and implementation of such a strategy.

You can also apply the methodology to [Establish clear business commitments](#).

# Azure management guide: Before you start

5/12/2020 • 2 minutes to read • [Edit Online](#)

## Before you start

The Azure Management Guide helps Azure customers create a management baseline to establish resource consistency across Azure. This guide outlines the basic tools needed for any Azure production environments, especially environments that host sensitive data. For more information, best practices, and considerations related to preparing your cloud environment, see the [readiness section](#) of the Cloud Adoption Framework.

## Scope of this guide

This guide teaches you how to establish tooling for a management baseline. It also outlines ways to extend the baseline or build resiliency beyond the baseline.

- **Inventory and visibility:** Create an inventory of assets across multiple clouds. Develop visibility into the run state of each asset.
- **Operational compliance:** Establish controls and processes to ensure each state is properly configured and running in a well-governed environment.
- **Protect and recover:** Ensure all managed assets are protected and can be recovered using baseline management tooling.
- **Enhanced baseline options:** Evaluate common additions to the baseline that might meet business needs.
- **Platform operations:** Extend the management baseline with a well-defined service catalog and centrally managed platforms.
- **Workload operations:** Extend the management baseline to include a focus on mission-critical workloads.

## Management baseline

A management baseline is the minimum set of tools and processes that should be applied to every asset in an environment. Several additional options can be included in the management baseline. The next few articles accelerate cloud management capabilities by focusing on the minimum options necessary instead of on all of the available options.

The next step is [Inventory and visibility](#).

This guide provides interactive steps that let you try features as they're introduced. To come back to where you left off, use the breadcrumb for navigation.

# Inventory and visibility in Azure

11/9/2020 • 3 minutes to read • [Edit Online](#)

*Inventory and visibility* is the first of three disciplines in a cloud management baseline.



## Basic level of cloud management for non-critical, production workloads

This discipline comes first because collecting proper operational data is vital when you make decisions about operations. Cloud management teams must understand what is managed and how well those assets are operated. This article describes the different tools that provide both an inventory and visibility into the inventory's run state.

For any enterprise-grade environment, the following table outlines the suggested minimum for a management baseline.

PROCESS	TOOL	PURPOSE
Monitor health of Azure services	Azure Service Health	Health, performance, and diagnostics for services running in Azure
Log centralization	Log Analytics	Central logging for all visibility purposes
Monitoring centralization	Azure Monitor	Central monitoring of operational data and trends
Virtual machine inventory and change tracking	Azure Change Tracking and Inventory	Inventory VMs and monitor changes for guest OS level
Subscription Monitoring	Azure Activity Log	Monitoring change at the subscription level
Guest OS monitoring	Azure Monitor for VMs	Monitoring changes and performance of VMs
Network monitoring	Azure Network Watcher	Monitoring network changes and performance

PROCESS	TOOL	PURPOSE
DNS monitoring	DNS Analytics	Security, performance, and operations of DNS

## Azure Service Health

- [Azure Service Health](#)

Azure Service Health provides a personalized view of the health of your Azure services and regions. Information about active issues is posted to Azure Service Health to help you understand the effect on your resources. Regular updates keep you informed as issues are resolved.

We also publish planned maintenance events to Azure Service Health so you'll know about changes that can affect resource availability. Set up Service Health alerts to notify you when service issues, planned maintenance, or other changes might affect your Azure services and regions.

Azure Service Health includes:

- **Azure status:** A global view of the health of Azure services.
- **Service health:** A personalized view of the health of your Azure services.
- **Resource health:** A deeper view of the health of your individual resources.

### Action

To set up a Service Health alert:

1. Go to [Service Health](#).
2. Select [Health alerts](#).
3. Create a Service Health alert.



To set up Service Health alerts, go to the [Azure portal](#).

### Learn more

For more information, see [Azure Service Health](#).

## Log Analytics

- [Log Analytics](#)

A [Log Analytics workspace](#) is a unique environment for storing Azure Monitor log data. Each workspace has its own data repository and configuration. Data sources and solutions are configured to store their data in particular workspaces. Azure monitoring solutions require all servers to be connected to a workspace, so that their log data can be stored and accessed.

### Action



### Learn more

To learn more, see the [Log Analytics workspace creation documentation](#).

## Azure Monitor

- [Azure Monitor](#)

Azure Monitor provides a single unified hub for all monitoring and diagnostics data in Azure and gives you visibility across your resources. With Azure Monitor, you can find and fix problems and optimize performance. You can also understand customer behavior.

- **Monitor and visualize metrics.** Metrics are numerical values available from Azure resources. They help you understand the health of your systems. Customize charts for your dashboards, and use workbooks for reporting.
- **Query and analyze logs.** Logs include activity logs and diagnostic logs from Azure. Collect additional logs from other monitoring and management solutions for your cloud or on-premises resources. Log Analytics provides a central repository to aggregate all of this data. From there, you can run queries to help troubleshoot issues or to visualize data.
- **Set up alerts and actions.** Alerts notify you of critical conditions. Corrective actions can be taken based on triggers from metrics, logs, or service-health issues. You can set up different notifications and actions and can also send data to your IT service management tools.

## Action



Start monitoring your:

- [Applications](#)
- [Containers](#)
- [Virtual machines](#)
- [Networks](#)

To monitor other resources, find additional solutions in Azure Marketplace.

To explore Azure Monitor, go to the [Azure portal](#).

## Learn more

To learn more, see [Azure Monitor documentation](#).

## Onboard solutions

- [Onboard solutions](#)

To enable solutions, you need to configure the Log Analytics workspace. Onboarded Azure VMs and on-premises servers get the solutions from the Log Analytics workspaces they're connected to.

There are two approaches to onboarding:

- [Single VM](#)
- [Entire subscription](#)

Each article guides you through a series of steps to onboard these solutions:

- Update Management
- Change Tracking and Inventory
- Azure Activity Log
- Azure Log Analytics Agent Health
- Antimalware Assessment
- Azure Monitor for VMs

- Azure Security Center

Each of the previous steps helps establish inventory and visibility.

# Operational compliance in Azure

11/9/2020 • 3 minutes to read • [Edit Online](#)

*Operational compliance* is the second discipline in any cloud management baseline.



Basic level of cloud management for non-critical, production workloads

Improving operational compliance reduces the likelihood of an outage related to configuration drift or vulnerabilities related to systems being improperly patched.

For any enterprise-grade environment, this table outlines the suggested minimum for a management baseline.

PROCESS	TOOL	PURPOSE
Patch management	Update Management	Management and scheduling of updates
Policy enforcement	Azure Policy	Policy enforcement to ensure environment and guest compliance
Environment configuration	Azure Blueprints	Automated compliance for core services
Resource Configuration	Desired State Configuration	Automated configuration on Guest OS and some aspects of the environment

## Update Management

- [Update Management](#)

Computers that are managed by Update Management use the following configurations to do assessment and update deployments:

- Microsoft Monitoring Agent (MMA) for Windows or Linux.
- PowerShell Desired State Configuration (DSC) for Linux.
- Azure Automation Hybrid Runbook Worker.
- Microsoft Update or Windows Server Update Services (WSUS) for Windows computers.

For more information, see [Update Management solution](#).

#### WARNING

Before using Update Management, you must onboard virtual machines or an entire subscription into Log Analytics and Azure Automation.

There are two approaches to onboarding:

- Single VM
- Entire subscription

You should follow one before proceeding with Update Management.

## Manage updates

To apply a policy to a resource group:

1. Go to [Azure Automation](#).
2. Select **Automation accounts**, and choose one of the listed accounts.
3. Go to **Configuration Management**.
4. **Inventory**, **Change Management**, and **State Configuration** can be used to control the state and operational compliance of the managed VMs.

ASSIGN  
POLICY

## Azure Policy

- [Azure Policy](#)

Azure Policy is used throughout governance processes. It's also highly valuable within cloud management processes. Azure Policy can audit and remediate Azure resources and can also audit settings inside a machine. The validation is performed by the Guest Configuration extension and client. The extension, through the client, validates settings like:

- Operating system configuration.
- Application configuration or presence.
- Environment settings.

Azure Policy Guest Configuration currently only audits settings inside the machine. It doesn't apply configurations.

### Action

Assign a built-in policy to a management group, subscription, or resource group.

ASSIGN  
POLICY

### Apply a policy

To apply a policy to a resource group:

1. Go to [Azure Policy](#).
2. Select **Assign a policy**.

### Learn more

To learn more, see:

- [Azure Policy](#)

- [Azure Policy: Guest configuration](#)
- [Cloud Adoption Framework: Policy enforcement decision guide](#)

## Azure Blueprints

- [Azure Blueprints](#)

With Azure Blueprints, cloud architects and central information-technology groups can define a repeatable set of Azure resources. These resources implement and adhere to an organization's standards, patterns, and requirements.

With Azure Blueprints, development teams can rapidly build and stand up new environments. Teams can also trust they're building within organizational compliance. They do so by using a set of built-in components like networking to speed up development and delivery.

Blueprints are a declarative way to orchestrate the deployment of different resource templates and other artifacts like:

- Role assignments.
- Policy assignments.
- Azure Resource Manager templates.
- Resource groups.

Applying a blueprint can enforce operational compliance in an environment if this enforcement isn't done by the cloud governance team.

### Create a blueprint

To create a blueprint:

1. Go to [Blueprints: Getting started](#).
2. On the **Create a Blueprint** pane, select **Create**.
3. Filter the list of blueprints to select the appropriate blueprint.
4. In the **Blueprint name** box, enter the blueprint name.
5. Select **Definition location**, and choose the appropriate location.
6. Select **Next : Artifacts >>**, and review the artifacts included in the blueprint.
7. Select **Save draft**.



1. Go to [Blueprints: Getting started](#).
2. On the **Create a Blueprint** pane, select **Create**.
3. Filter the list of blueprints to select the appropriate blueprint.
4. In the **Blueprint name** box, enter the blueprint name.
5. Select **Definition location**, and choose the appropriate location.
6. Select **Next : Artifacts >>**, and review the artifacts included in the blueprint.
7. Select **Save draft**.

### Publish a blueprint

To publish blueprint artifacts to your subscription:

1. Go to [Blueprints - Blueprint definitions](#).
2. Select the blueprint you created in the previous steps.
3. Review the blueprint definition, then select **Publish blueprint**.

4. In the **Version** box, enter a version like "1.0".

5. In the **Change notes** box, enter your notes.

6. Select **Publish**.

B  
L  
U  
E  
P  
R  
I  
N  
T

D  
E  
F  
I  
N  
I  
T  
I  
O  
N  
S

1. In the Azure portal, go to [Blueprints: Blueprint definitions](#).
2. Select the blueprint you created in the previous steps.
3. Review the blueprint definition, then select **Publish blueprint**.
4. In the **Version** box, enter a version like "1.0".
5. In the **Change notes** box, enter your notes.
6. Select **Publish**.

## Learn more

To learn more, see:

- [Azure Blueprints](#)
- [Cloud Adoption Framework: Resource consistency decision guide](#)
- [Standards-based blueprints samples](#)

# Protect and recover in Azure

11/9/2020 • 2 minutes to read • [Edit Online](#)

*Protect and recover* is the third and final discipline in any cloud-management baseline.



Basic level of cloud management for non-critical, production workloads

In [Operational compliance in Azure](#) the objective is to reduce the likelihood of a business interruption. The current article aims to reduce the duration and impact of outages that can't be prevented.

For any enterprise-grade environment, this table outlines the suggested minimum for any management baseline:

PROCESS	TOOL	PURPOSE
Protect data	Azure Backup	Back up data and virtual machines in the cloud.
Protect the environment	Azure Security Center	Strengthen security and provide advanced threat protection across your hybrid workloads.

## Azure Backup

- [Azure Backup](#)

With Azure Backup, you can back up, protect, and recover your data in the Microsoft cloud. Azure Backup replaces your existing on-premises or offsite backup solution with a cloud-based solution. This new solution is reliable, secure, and cost competitive. Azure Backup can also help protect and recover on-premises assets through one consistent solution.

For data present in Azure, Azure Backup offer varied levels of protection. For eg: For backing up key cloud infrastructure pieces such as Azure Virtual machines and Azure Files, it offers [Azure virtual machine backup](#) and [Azure files backup](#). For more critical components such as databases running in Azure Virtual machines, it offers dedicated database backup solutions for [MS SQL](#) and [SAP HANA](#) with far lower RPO.

To get a glimpse of how easy it is to enable backup with Azure Backup, look at the section below to enable backup for Azure Virtual machines

## Enable backup for an Azure VM

1. In the Azure portal, select **Virtual machines**, then select the VM you want to backup.
2. On the **Operations** pane, select **Backup**.
3. Create or select an existing Azure Recovery Services vault.
4. Select **Create (or edit) a new policy**.
5. Configure the schedule and retention period.
6. Select **OK**.
7. Select **Enable backup**.

GO TO VIRTUAL  
MACHINES

For more details about Azure Backup and its varied offering, refer to this [Overview](#) section

## Azure Site Recovery

- [Azure Site Recovery](#)

Azure Site Recovery is a critical component in your disaster recovery strategy.

Site Recovery replicates VMs and workloads that are hosted in a primary Azure region. It replicates them to a copy that is hosted in a secondary region. When an outage occurs in your primary region, you fail over to the copy running in the secondary region. You then continue to access your applications and services from there. This proactive approach to recovery can significantly reduce recovery times. When the recovery environment is no longer needed, production traffic can fall back to the original environment.

### Replicate an Azure VM to another region with Site Recovery

The following steps outline the process to use Site Recovery for Azure-to-Azure replication, which is replication of an Azure VM to another region.

#### TIP

Depending on your scenario, the exact steps might differ slightly.

## Enable replication for the Azure VM

1. In the Azure portal, select **Virtual machines**, then select the VM you want to replicate.
2. On the **Operations** pane, select **Disaster recovery**.
3. Select **Configure disaster recovery > Target region**, and choose the target region to which you'll replicate.
4. For this quickstart, accept the default values for all other options.
5. Select **Enable replication**, which starts a job to enable replication for the VM.

GO TO VIRTUAL  
MACHINES

## Verify settings

After the replication job has finished, you can check the replication status, verify replication health, and test the deployment.

1. In the VM menu, select **Disaster recovery**.
2. Verify replication health, the recovery points that have been created, and source and target regions on the map.

GO TO VIRTUAL  
MACHINES

**Learn more**

- [Azure Site Recovery overview](#)
- [Replicate an Azure VM to another region](#)

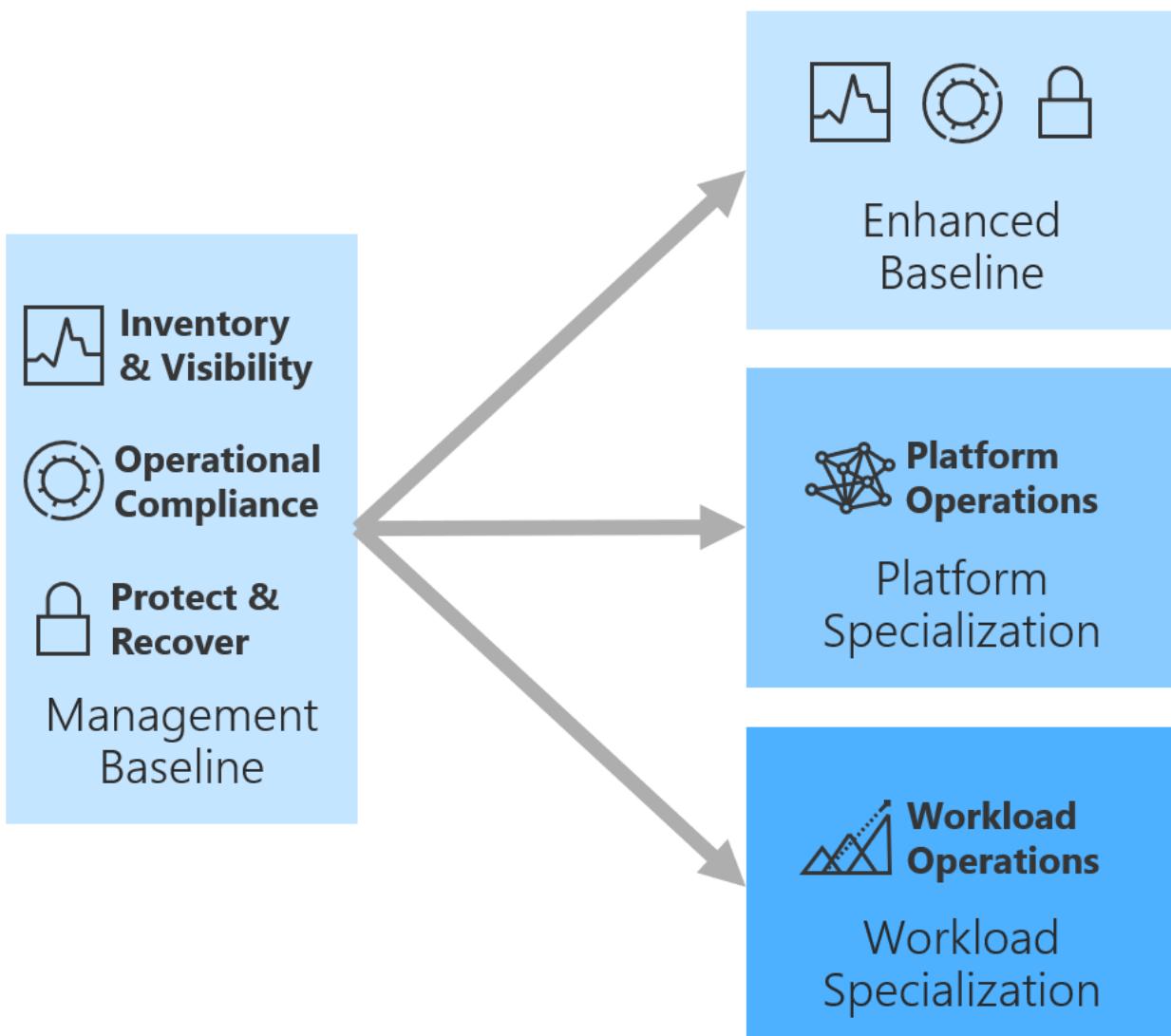
# Enhanced management baseline in Azure

11/9/2020 • 4 minutes to read • [Edit Online](#)

The first three cloud management disciplines describe a management baseline. The preceding articles in this guide outline a minimum viable product (MVP) for cloud management services, which is referred to as a management baseline. This article outlines a few common improvements to the baseline.

The purpose of a management baseline is to create a consistent offering that provides a minimum level of business commitment for **all** supported workloads. With this baseline of common, repeatable management offerings, the team can deliver highly optimized operational management with minimal deviation.

However, you might need a greater commitment to the business beyond the standard offering. The following image and list show three ways to go beyond the management baseline.



- **Enhanced management baseline:**

- Add enhancements to the management baseline, when the majority of workloads in the portfolio have a shared requirement.
- Improved business commitments using additional cloud-native operations tools and processes.
- Baseline enhancements should have no impact on the architecture of specific workloads.

- **Workload operations:**

- Largest per-workload operations investment.
- Highest degree of resiliency.
- Suggested for the approximately 20 percent of workloads that drive business value.
- Typically reserved for high-criticality or mission-critical workloads.

- **Platform operations:**

- Operations investment is spread across many workloads.
- Resiliency improvements affect all workloads that use the defined platform.
- Suggested for the approximately 20 percent of platforms that have highest criticality.
- Typically reserved for medium-criticality to high-criticality workloads.

Both workload operations and platform operations require changes to design and architecture principles. Those changes can take time and might result in increased operating expenses. To reduce the number of workloads that require such investments, an enhanced management baseline can provide enough of an improvement to the business commitment.

This table outlines a few processes, tools, and potential effects common in customers' enhanced management baselines:

DISCIPLINE	PROCESS	TOOL	POTENTIAL IMPACT	LEARN MORE
Inventory and visibility	Service change tracking	Azure Resource Graph	Greater visibility into changes to Azure services might help detect negative effects sooner or remediate faster.	<a href="#">Overview of Azure Resource Graph</a>
Inventory and visibility	IT service management (ITSM) integration	IT Service Management Connector	Automated ITSM connection creates awareness sooner.	<a href="#">IT Service Management Connector (ITSMC)</a>
Operational compliance	Operations automation	Azure Automation	Automate operational compliance for faster and more accurate response to change.	See the following sections
Operational compliance	Performance automation	Azure Automation	Automate operational compliance with performance expectations to resolve common resource specific scaling or sizing issues.	See the following sections
Operational compliance	Multicloud operations	Azure Automation Hybrid Runbook Worker	Automate operations across multiple clouds.	<a href="#">Hybrid Runbook Worker overview</a>
Operational compliance	Guest automation	Desired State Configuration (DSC)	Code-based configuration of guest operating systems to reduce errors and configuration drift.	<a href="#">DSC Overview</a>

DISCIPLINE	PROCESS	TOOL	POTENTIAL IMPACT	LEARN MORE
Protect and recover	Breach notification	Azure Security Center	Extend protection to include security-breach recovery triggers.	See the following sections

## Azure Automation

- [Azure Automation](#)

Azure Automation provides a centralized system for the management of automated controls. In Azure Automation, you can run simple remediation, scale, and optimization processes in response to environmental metrics. These processes reduce the overhead associated with manual incident processing.

Most importantly, automated remediation can be delivered in near-real-time, significantly reducing interruptions to business processes. A study of the most common business interruptions identifies activities within your environment that could be automated.

### Runbooks

The basic unit of code for delivering automated remediation is a runbook. Runbooks contain the instructions for remediating or recovering from an incident.

To create or manage runbooks:

1. Go to [Azure Automation](#).
2. Select **Automation accounts** and choose one of the listed accounts.
3. Go to **Process automation**.
4. With the options presented, you can create or manage runbooks, schedules, and other automated remediation functionality.

GO TO AZURE  
AUTOMATION

## Azure Security Center

- [Azure Security Center](#)

Azure Security Center also plays an important part in your protect-and-recover strategy. It can help you monitor the security of your machines, networks, storage, data services, and applications.

Azure Security Center provides advanced threat detection by using machine learning and behavioral analytics to help identify active threats targeting your Azure resources. It also provides threat protection that blocks malware and other unwanted code, and it reduces the surface area exposed to brute force and other network attacks.

When Azure Security Center identifies a threat, it triggers a security alert with steps you need for responding to an attack. It also provides a report with information about the detected threat.

Azure Security Center is offered in two tiers: Free and Standard. Features like security recommendations are available in the Free tier. The Standard tier provides additional protection like advanced threat detection and protection across hybrid cloud workloads.

### Action

**Try Standard tier for free for your first 30 days**

After you enable and configure security policies for a subscription's resources, you can view the security state of your resources and any issues on the **Prevention** pane. You can also view a list of those issues on the

**Recommendations tile.**

EXPLORE AZURE SECURITY  
CENTER

To explore Azure Security Center, go to the [Azure portal](#).

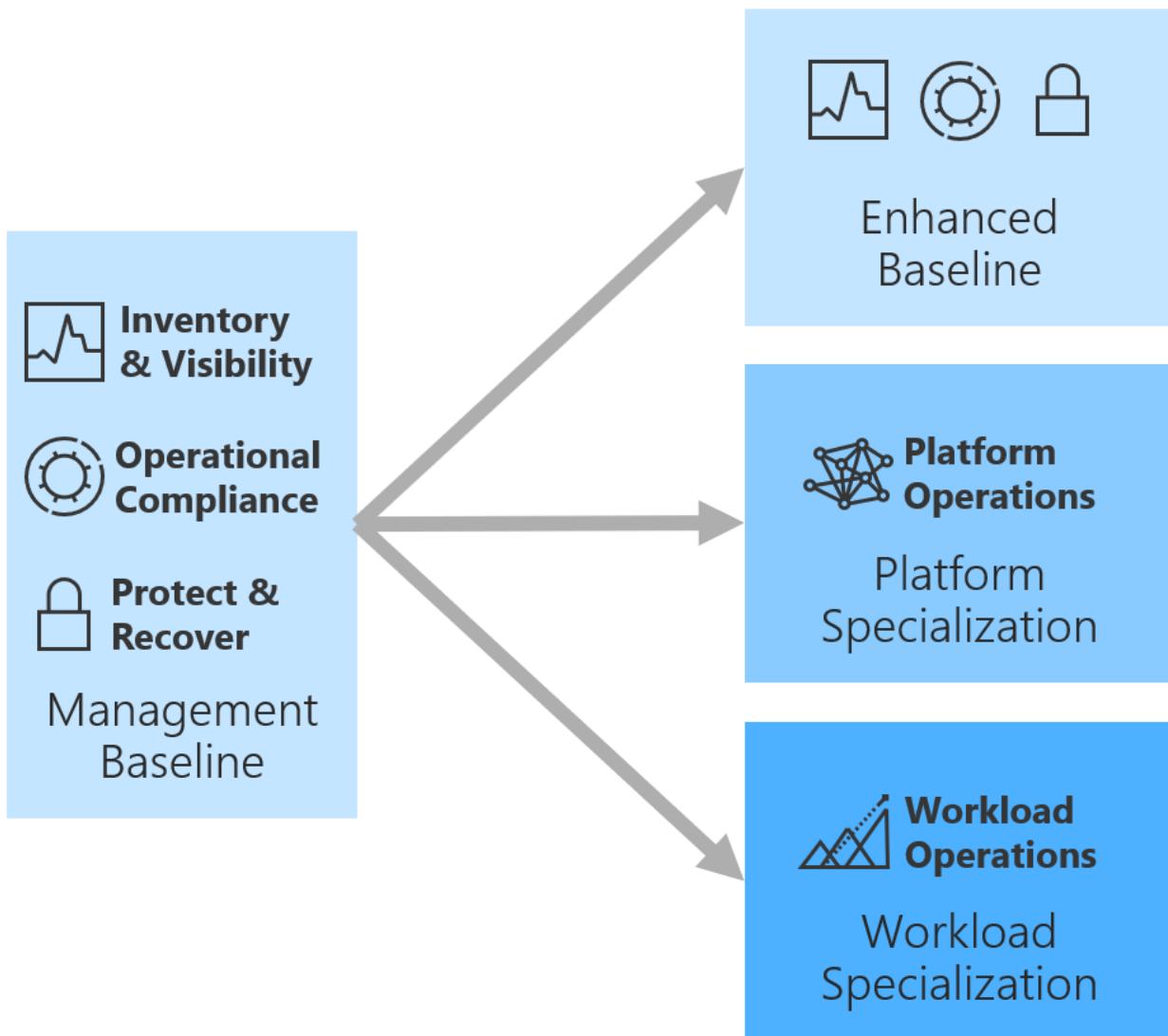
**Learn more**

To learn more, see [Azure Security Center documentation](#).

# Platform specialization for cloud management

11/9/2020 • 5 minutes to read • [Edit Online](#)

Much like the enhanced management baseline, platform specialization is extension beyond the standard management baseline. See the following image and list that show the ways to expand the management baseline. This article addresses the platform specialization options.



- **Workload operations:** The largest per-workload operations investment and the highest degree of resiliency. We suggest workload operations for the approximately 20% of workloads that drive business value. This specialization is usually reserved for high criticality or mission-critical workloads.
- **Platform operations:** Operations investment is spread across many workloads. Resiliency improvements affect all workloads that use the defined platform. We suggest platform operations for the approximately 20% of platforms that have the highest criticality. This specialization is usually reserved for medium to high criticality workloads.
- **Enhanced management baseline:** The relatively lowest operations investment. This specialization slightly improves business commitments by using additional cloud-native operations tools and processes.

Both workload and platform operations require changes to design and architecture principles. Those changes can take time and might result in increased operating expenses. To reduce the number of workloads requiring such

investments, an enhanced management baseline might provide enough of an improvement to the business commitment.

This table outlines a few common processes, tools, and potential effects common in customers' enhanced management baselines:

PROCESS	TOOL	PURPOSE	SUGGESTED MANAGEMENT LEVEL
Improve system design	Microsoft Azure Well-Architected Framework	Improving the architectural design of the platform to improve operations	N/A
Automate remediation	Azure Automation	Responding to advanced platform data with platform-specific automation	Platform operations
Service catalog	Managed applications center	Providing a self-service catalog of approved solutions that meet organizational standards	Platform operations
Container performance	Azure Monitor for containers	Monitoring and diagnostics of containers	Platform operations
Platform as a service (PaaS) data performance	Azure SQL Analytics	Monitoring and diagnostics for PaaS databases	Platform operations
Infrastructure as a service (IaaS) data performance	SQL Server Health Check	Monitoring and diagnostics for IaaS databases	Platform operations

## High-level process

Platform specialization consists of a disciplined execution of the following four processes in an iterative approach. Each process is explained in more detail in later sections of this article.

- **Improve system design:** Improve the design of common systems or platforms to effectively minimize interruptions.
- **Automate remediation:** Some improvements aren't cost effective. In such cases, it might make more sense to automate remediation and reduce the effect of interruptions.
- **Scale the solution:** As systems design and automated remediation are improved, those changes can be scaled across the environment through the service catalog.
- **Continuous improvement:** Different monitoring tools can be used to discover incremental improvements. These improvements can be addressed in the next pass of system design, automation, and scale.

## Improve system design

- [Improve system design](#)

Improving system design is the most effective approach to improving operations of any common platform. Through system-design improvements, stability can increase and business interruptions can decrease. Design of individual systems is beyond the scope of the environment view that's taken throughout the Cloud Adoption Framework.

As a complement to this framework, the [Microsoft Azure Well-Architected Framework](#) provides guiding tenets for improving the quality of a platform or a specific workload. The framework focuses on improvement across five

pillars of architecture excellence:

- **Cost optimization:** Manage costs to maximize the value delivered.
- **Operational excellence:** Follow operational processes that keep a system running in production.
- **Performance efficiency:** Scale systems to adapt to changes in load.
- **Reliability:** Design systems to recover from failures and continue to function.
- **Security:** Protect applications and data from threats.

Technical debt and architectural flaws cause most business interruptions. For existing deployments, you can view system-design improvements as payments against existing technical debt. For new deployments, you can view those improvements as avoidance of technical debt.

The following **Automated remediation** tab shows ways to remediate technical debt that can't or shouldn't be addressed.

Learn more about the [Microsoft Azure Well-Architected Framework](#) to improve system design.

As system design improves, return to this article to find new opportunities to improve and scale those improvements across your environment.

## Automated remediation

- [Automated remediation](#)

Some technical debt can't be addressed. Resolution might be too expensive to correct or might be planned but have a long project duration. The business interruption might not have a significant business effect. Or the business priority might be to recover quickly instead of investing in resiliency.

When resolution of technical debt isn't the desired approach, automated remediation is commonly the next step. Using Azure Automation and Azure Monitor to detect trends and provide automated remediation is the most common approach to automated remediation.

For guidance on automated remediation, see [Azure Automation and alerts](#).

## Scale the solution with a service catalog

- [Scale the solution with a service catalog](#)

A well-managed service catalog is the cornerstone of platform specialization and platform operations. Use of a catalog is how improvements to systems design and remediation are scaled across an environment.

The cloud platform team and cloud automation team align to create repeatable solutions to the most common platforms in any environment. But if those solutions aren't consistently used, cloud management can provide little more than a baseline offering.

To maximize adoption and minimize maintenance overhead of any optimized platform, you should add the platform to an Azure service catalog. You can deploy each application in the catalog for internal consumption via the service catalog or as a marketplace offering for external consumers.

For instructions on publishing to a service catalog, see the article series on [publishing to a service catalog](#).

### Deploy applications from the service catalog

1. In the Azure portal, go to [Managed applications center \(preview\)](#).
2. On the **Browse** pane, select **Service Catalog applications**.
3. Select **+ Add** to choose an application definition from your company's service catalog.

Any managed applications you're servicing are displayed.

GO TO VIRTUAL  
MACHINES

## Manage service catalog applications

1. In the Azure portal, go to **Managed applications center (preview)**.
2. On the **Service** pane, select **Service Catalog applications**.

Any managed applications you're servicing are displayed.

GO TO VIRTUAL  
MACHINES

## Continuous improvement

- [Continuous improvement](#)

Platform specialization and platform operations both depend on strong feedback loops among adoption, platform, automation, and management teams. Grounding those feedback loops in data helps each team make wise decisions. For platform operations to achieve long-term business commitments, it's important to use insights specific to the centralized platform.

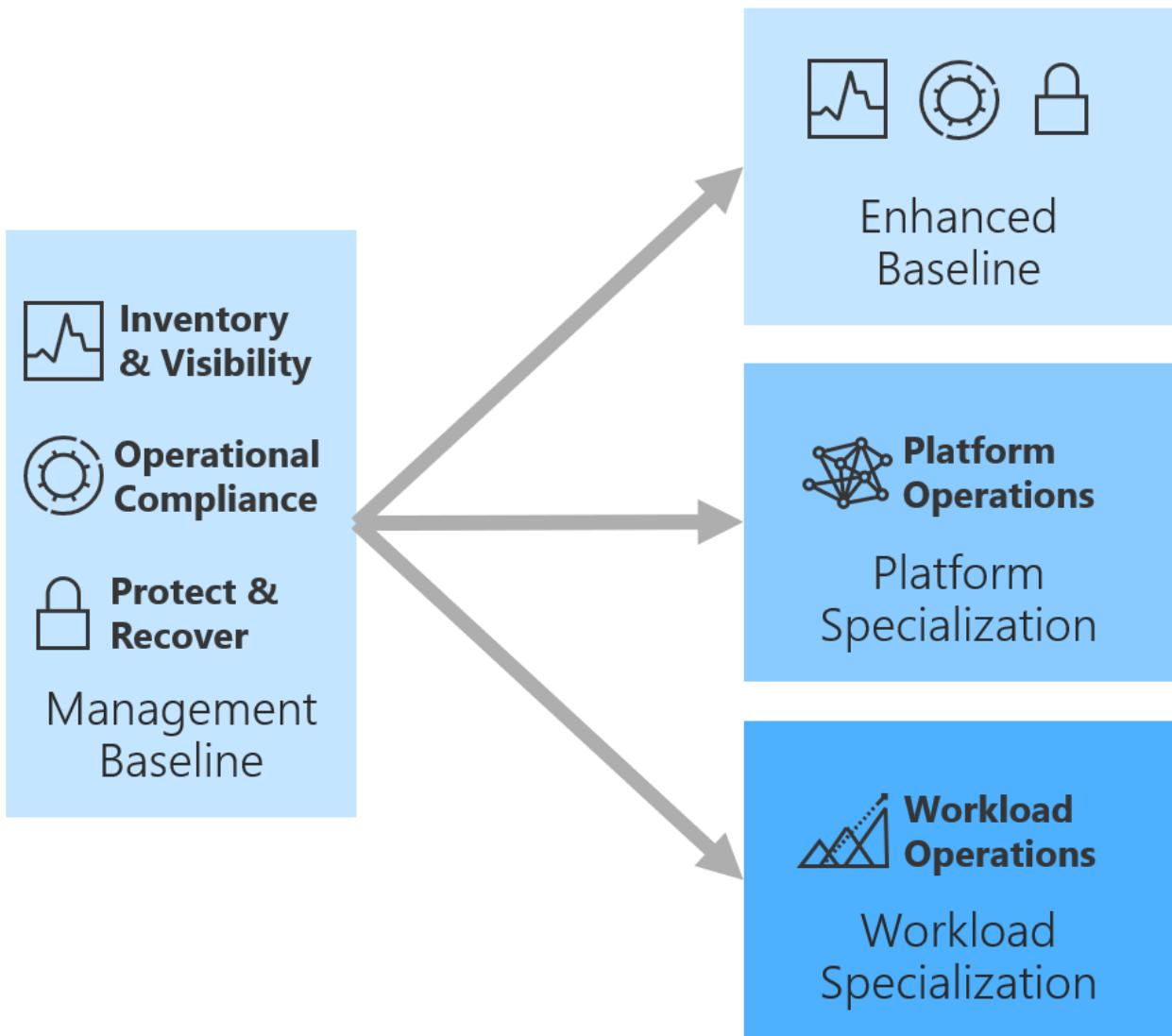
Containers and SQL Server are the two most common centrally managed platforms. These articles can help you get started with continuous-improvement data collection on those platforms:

- [Container performance](#)
- [PaaS database performance](#)
- [IaaS database performance](#)

# Workload specialization for cloud management

11/9/2020 • 2 minutes to read • [Edit Online](#)

Workload specialization builds on the concepts outlined in [Platform Specialization](#).



- **Workload operations:** The largest per-workload operations investment and highest degree of resiliency. We suggest workload operations for the approximately 20% of workloads that drive business value. This specialization is usually reserved for high criticality or mission-critical workloads.
- **Platform operations:** Operations investment is spread across many workloads. Resiliency improvements affect all workloads that use the defined platform. We suggest platform operations for the approximately 20% of platforms that have the highest criticality. This specialization is usually reserved for medium to high criticality workloads.
- **Enhanced management baseline:** The relatively lowest operations investment. This specialization slightly improves business commitments by using additional cloud-native operations tools and processes.

## High-level process

Workload specialization consists of a disciplined execution of the following four processes in an iterative approach. Each process is explained in more detail in [Platform Specialization](#).

- **Improve system design:** Improve the design of a specific workload to effectively minimize interruptions.
- **Automate remediation:** Some improvements aren't cost effective. In such cases, it might make more sense to automate remediation and reduce the effect of interruptions.
- **Scale the solution:** As you improve systems design and automated remediation, you can scale those changes across the environment through the service catalog.
- **Continuous improvement:** You can use different monitoring tools to discover incremental improvements. These improvements can be addressed in the next pass of system design, automation, and scale.

## Cultural change

Workload specialization often triggers a cultural change in traditional IT build processes that focus on delivering a management baseline, enhanced baselines, and platform operations. Those types of offerings can be scaled across the environment. Workload specialization is similar in execution to platform specialization. But unlike common platforms, the specialization required by individual workloads often doesn't scale.

When workload specialization is required, operational management commonly evolves beyond a centralized IT perspective. The approach suggested in Cloud Adoption Framework is a distribution of cloud management functionality.

In this model, operational tasks like monitoring, deployment, DevOps, and other innovation-focused functions shift to an application-development or business-unit organization. The cloud platform team and the core cloud monitoring team still delivers on the management baseline across the environment.

Those centralized teams also guide and instruct workload-specialized teams on operations of their workloads. But the day-to-day operational responsibility falls on a cloud management team that is managed outside of IT. This type of distributed control is one of the primary indicators of maturity in a cloud center of excellence.

## Beyond platform specialization: Application Insights

Greater detail on the specific workload is required to provide clear workload operations. During the continuous improvement phase, Application Insights will be a necessary addition to the cloud management toolchain.

REQUIREMENT	TOOL	PURPOSE
Application monitoring	Application Insights	Monitoring and diagnostics for apps
Performance, availability, and usage	Application Insights	Advanced application monitoring with the application dashboard, composite maps, usage, and tracing

### Deploy Application Insights

1. In the Azure portal, go to [Application Insights](#).
2. Select + Add to create an Application Insights resource to monitor your live web application.
3. Follow the on-screen prompts.

See the [Azure Monitor Application Insights hub](#) for guidance on configuring your application for monitoring.



### Monitor performance, availability, and usage

1. In the Azure portal, search for [Application Insights](#).
2. Choose one of the Application Insights resources from the list.

Application Insights contains different kinds of options for monitoring performance, availability, usage, and

dependencies. Each of these views of the application data provides clarity into the continuous-improvement feedback loop.

MONITOR  
APPLICATIONS

# Establish operational management practices in the cloud

11/9/2020 • 2 minutes to read • [Edit Online](#)

Cloud adoption is a catalyst for enabling business value. However, real business value is realized through ongoing, stable operations of the technology assets deployed to the cloud. This section of the Cloud Adoption Framework guides you through various transitions into operational management in the cloud.

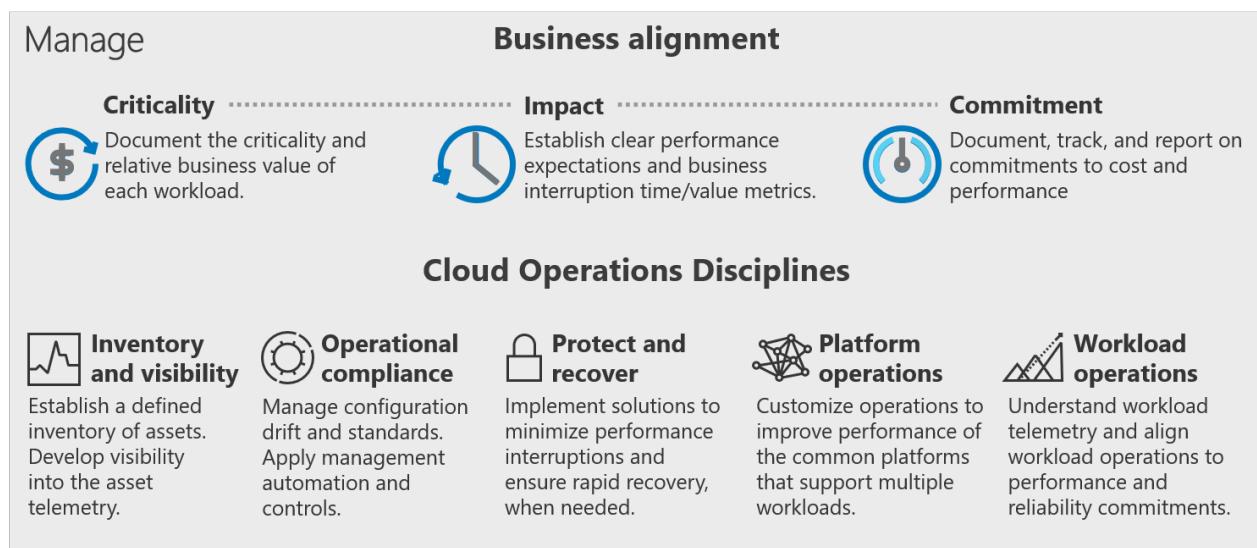
## Actionable best practices

Modern operations management solutions create a multicloud view of operations. Assets managed through the following best practices may live in the cloud, in an existing datacenter, or even in a competing cloud provider. Currently, the framework includes two best-practices references to guide operations management maturity in the cloud:

- [Azure server management](#): An onboarding guide to incorporating the cloud-native tools and services needed to manage operations.
- [Hybrid monitoring](#): Many customers have already made a substantial investment in System Center Operations Manager. For those customers, this guide to hybrid monitoring can help them compare and contrast the cloud-native reporting tools with Operations Manager tooling. This comparison makes it easier to decide which tools to use for operational management.

## Cloud operations

Both of these best practices build toward a future-state methodology for operations management, as illustrated in the following diagram:



**Business alignment:** In the Manage methodology, all workloads are classified by criticality and business value. That classification can then be measured through an impact analysis, which calculates the lost value associated with performance degradation or business interruptions. Using that tangible revenue impact, cloud operations teams can work with the business to establish a commitment that balances cost and performance.

**Cloud operations disciplines:** After the business is aligned, it's much easier to track and report on the proper disciplines of cloud operations for each workload. Making decisions along each discipline can then be converted to commitment terms that can be easily understood by the business. This collaborative approach makes the

business stakeholder a partner in finding the right balance between cost and performance.

- **Inventory and visibility:** At a minimum, operations management requires a means of inventorying assets and creating visibility into the run state of each asset.
- **Operational compliance:** Regular management of configuration, sizing, cost, and performance of assets is key to maintaining performance expectations.
- **Protect and recover:** Minimizing operational interruptions and expediting recovery help the business avoid performance losses and adverse revenue impacts. Detection and recovery are essential aspects of this discipline.
- **Platform operations:** All IT environments contain a set of commonly used platforms. Those platforms could include data stores such as SQL Server or Azure HDInsight. Other common platforms could include container solutions such as Azure Kubernetes Service (AKS). Regardless of the platform, platform operations maturity focuses on customizing operations based on how the common platforms are deployed, configured, and used by workloads.
- **Workload operations:** At the highest level of operational maturity, cloud operations teams can tune operations for critical workloads. For those workloads, available data can assist in automating the remediation, sizing, or protection of workloads based on their utilization.

Additional guidance, such as the [Design Review Framework \(Code name: Cloud Design Principles\)](#), can help you make detailed architectural decisions about each workload, within the previously described disciplines.

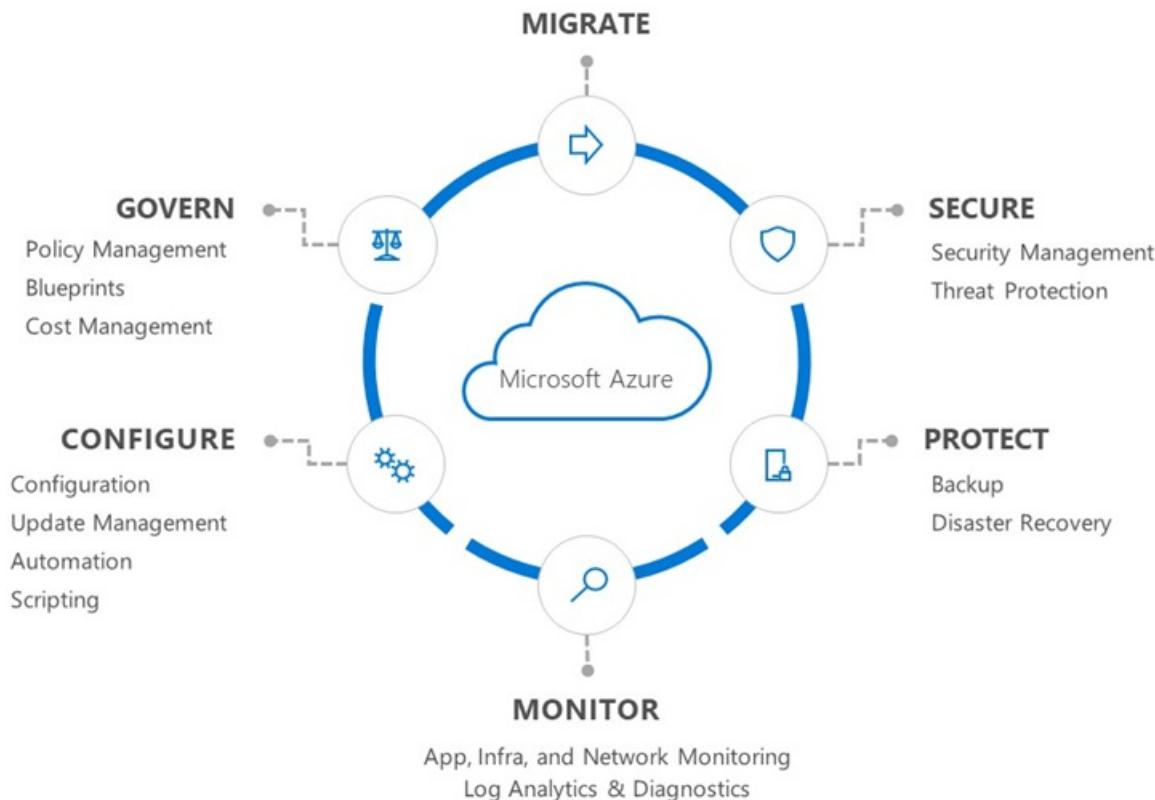
This section of the Cloud Adoption Framework will build on each of the preceding topics to help promote mature cloud operations within your organization.

# Overview of Azure server management services

11/9/2020 • 2 minutes to read • [Edit Online](#)

Azure server management services provide a consistent experience for managing servers at scale. These services cover both Linux and Windows operating systems. They can be used in production, development, and test environments. The server management services can support Azure IaaS virtual machines, physical servers, and virtual machines that are hosted on-premises or in other hosting environments.

The Azure server management services suite includes the services in the following diagram:



This section of the Microsoft Cloud Adoption Framework provides an actionable and prescriptive plan for deploying server management services in your environment. This plan helps orient you quickly to these services, guiding you through an incremental set of management stages for all environment sizes.

For simplicity, we've categorized this guidance into three stages:



## Why use Azure server management services?

Azure server management services offer the following benefits:

- **Native to Azure:** Server management services are built into and natively integrated with Azure Resource Manager. These services are continuously improved to provide new features and capabilities.
- **Windows and Linux:** Windows and Linux machines get the same consistent management experience.
- **Hybrid:** The server management services cover Azure IaaS virtual machines as well as physical and virtual servers that are hosted on-premises or in other hosting environments.
- **Security:** Microsoft devotes substantial resources to all forms of security. This investment not only protects the Azure infrastructure but also extends the resulting technologies and expertise to protect customers' resources wherever they reside.

## Next steps

Familiarize yourself with the [tools, services, and planning](#) involved with adopting the Azure server management suite.

[Prerequisite tools and planning](#)

# Phase 1: Prerequisite planning for Azure server management services

11/9/2020 • 6 minutes to read • [Edit Online](#)

In this phase, you'll become familiar with the Azure server management suite of services, and plan how to deploy the resources needed to implement these management solutions.

## Understand the tools and services

Review [Azure server management tools and services](#) for a detailed overview of:

- The management areas that are involved in ongoing Azure operations.
- The Azure services and tools that help support you in these areas.

You'll use several of these services together to meet your management requirements. These tools are referenced often throughout this guidance.

The following sections discuss the planning and preparation required to use these tools and services.

## Log Analytics workspace and Automation account planning

Many of the services you'll use to onboard Azure management services require a Log Analytics workspace and a linked Azure Automation account.

A [Log Analytics workspace](#) is a unique environment for storing Azure Monitor log data. Each workspace has its own data repository and configuration. Data sources and solutions are configured to store their data in particular workspaces. Azure monitoring solutions require all servers to be connected to a workspace, so that their log data can be stored and accessed.

Some of the management services require an [Azure Automation](#) account. You use this account, and the capabilities of Azure Automation, to integrate Azure services and other public systems to deploy, configure, and manage your server management processes.

The following Azure server management services require a linked Log Analytics workspace and Automation account:

- [Azure Update Management](#)
- [Change Tracking and Inventory](#)
- [Hybrid Runbook Worker](#)
- [Desired State Configuration](#)

The second phase of this guidance focuses on deploying services and automation scripts. It shows you how to create a Log Analytics workspace and an Automation account. This guidance also shows you how to use Azure Policy to ensure that new virtual machines are connected to the correct workspace.

The examples in this guidance assume a deployment that doesn't already have servers deployed to the cloud. To learn more about the principles and considerations involved in planning your workspaces, see [Manage log data and workspaces in Azure Monitor](#).

## Planning considerations

When preparing the workspaces and accounts that you need for onboarding management services, consider the

following issues:

- **Azure geographies and regulatory compliance:** Azure regions are organized into *geographies*. An [Azure geography](#) ensures that data residency, sovereignty, compliance, and resiliency requirements are honored within geographical boundaries. If your workloads are subject to data-sovereignty or other compliance requirements, workspace and Automation accounts must be deployed to regions within the same Azure geography as the workload resources they support.
- **Number of workspaces:** As a guiding principle, create the minimum number of workspaces required per Azure geography. We recommend at least one workspace for each Azure geography where your compute or storage resources are located. This initial alignment helps avoid future regulatory issues when you migrate data to different geographies.
- **Data retention and capping:** You may also need to take Data retention policies or data capping requirements into consideration when creating workspaces or Automation accounts. For more information about these principles, and for additional considerations when planning your workspaces, see [Manage log data and workspaces in Azure Monitor](#).
- **Region mapping:** Linking a Log Analytics workspace and an Azure Automation account is supported only between certain Azure regions. For example, if the Log Analytics workspace is hosted in the [East US](#) region, the linked Automation account must be created in the [East US 2](#) region to be used with management services. If you have an Automation account that was created in another region, it can't link to a workspace in [East US](#). The choice of deployment region can significantly affect Azure geography requirements. Consult the [region mapping table](#) to decide which region should host your workspaces and Automation accounts.
- **Workspace multihoming:** The Azure Log Analytics agent supports multihoming in some scenarios, but the agent faces several limitations and challenges when running in this configuration. Unless Microsoft has recommended it for your specific scenario, don't configure multihoming on the Log Analytics agent.

## Resource placement examples

There are several different models for choosing the subscription in which you place the Log Analytics workspace and Automation account. In short, place the workspace and Automation accounts in a subscription owned by the team that's responsible for implementing the Update Management service and the Change Tracking and Inventory service.

The following are examples of some ways to deploy workspaces and Automation accounts.

### Placement by geography

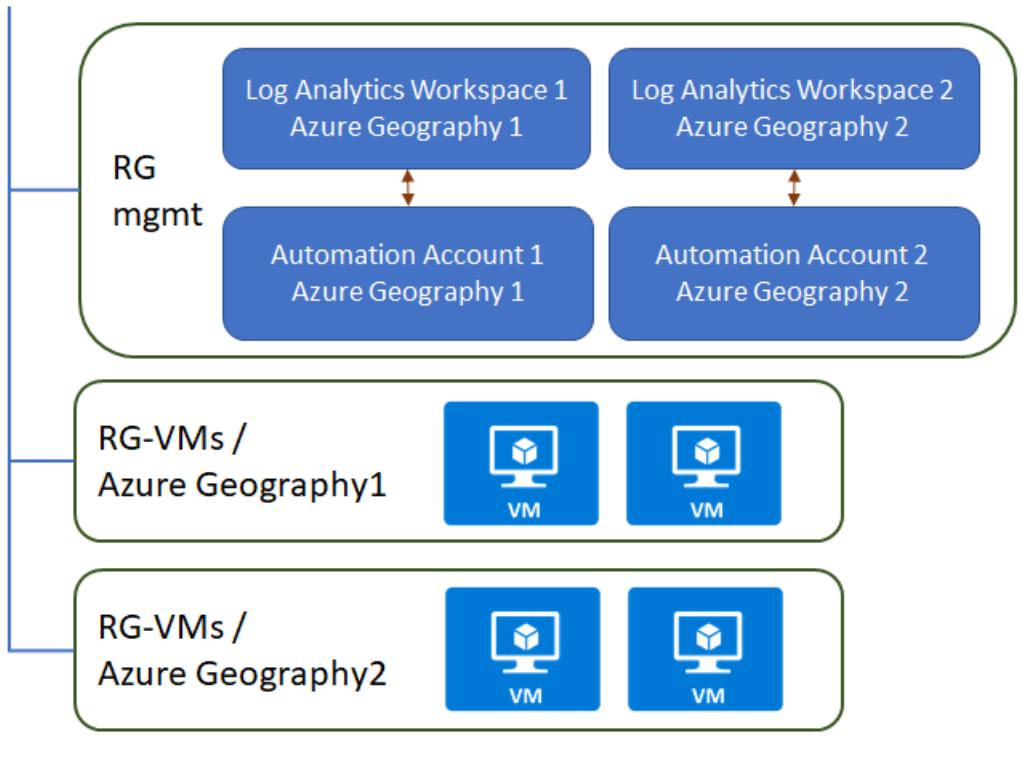
Small and midsize environments have a single subscription and several hundred resources that span multiple Azure geographies. For these environments, create one Log Analytics workspace and one Azure Automation account in each geography.

You can create a workspace and an Azure Automation account, as one pair, in each resource group. Then, deploy the pair in the corresponding geography to the virtual machines.

Alternatively, if your data-compliance policies don't dictate that resources reside in specific regions, you can create one pair to manage all the virtual machines. We also recommend that you place the workspace and Automation account pairs in separate resource groups to provide more granular role-based access control (RBAC).

The example in the following diagram has one subscription with two resource groups, each located in a different geography:

## Subscription



### Placement in a management subscription

Larger environments span multiple subscriptions and have a central IT team that owns monitoring and compliance. For these environments, create pairs of workspaces and Automation accounts in an IT management subscription. In this model, virtual-machine resources in a geography store their data in the corresponding geography workspace in the IT management subscription. If application teams need to run automation tasks but don't require linked workspace and Automation accounts, they can create separate Automation accounts in their own application subscriptions.

## Subscription (Management)



## Subscription (Application team)

RG - VMs /  
Azure Geography 1



## Subscription (Application team)

RG - VMs /  
Azure Geography 2



## Decentralized placement

In an alternative model for large environments, the application development team can be responsible for patching and management. In this case, place the workspace and Automation account pairs in the application team subscriptions alongside their other resources.

## Subscription (Application team)

RG - VMs /  
Azure Geography 1

Log Analytics Workspace 1  
Azure Geography 1



Automation Account 1  
Azure Geography 1



## Subscription (Application team)

RG - VMs /  
Azure Geography 2

Log Analytics Workspace 2  
Azure Geography 2



Automation Account 2  
Azure Geography 2



## Create a workspace and Automation account

After you've chosen the best way to place and organize workspace and account pairs, make sure that you've created these resources before starting the onboarding process. The automation examples later in this guidance create a workspace and Automation account pair for you. However, if you want to onboard by using the Azure portal and you don't have an existing workspace and Automation account pair, you'll need to create one.

To create a Log Analytics workspace by using the Azure portal, see [Create a workspace](#). Next, create a matching Automation account for each workspace by following the steps in [Create an Azure Automation account](#).

### NOTE

When you create an Automation account by using the Azure portal, the portal attempts by default to create Run As accounts for both Azure Resource Manager and the classic deployment model resources. If you don't have classic virtual machines in your environment and you're not the co-administrator on the subscription, the portal creates a Run As account for Resource Manager, but it generates an error when deploying the classic Run As account. If you don't intend to support classic resources, you can ignore this error.

You can also create Run As accounts by using [PowerShell](#).

## Next steps

Learn how to [onboard your servers](#) to Azure server management services.

[Onboard to Azure server management services](#)

# Phase 2: Onboarding Azure server management services

11/9/2020 • 2 minutes to read • [Edit Online](#)

After you're familiar with the [tools](#) and [planning](#) involved in Azure management services, you're ready for the second phase. Phase 2 provides step-by-step guidance for onboarding these services for use with your Azure resources. Start by evaluating this onboarding process before adopting it broadly in your environment.

## NOTE

The automation approaches discussed in later sections of this guidance are meant for deployments that don't already have servers deployed to the cloud. They require that you have the Owner role on a subscription to create all the required resources and policies. If you've already created Log Analytics workspaces and Automation accounts, we recommend that you pass these resources in the appropriate parameters when you start the example automation scripts.

## Onboarding processes

This section of the guidance covers the following onboarding processes for both Azure virtual machines and on-premises servers:

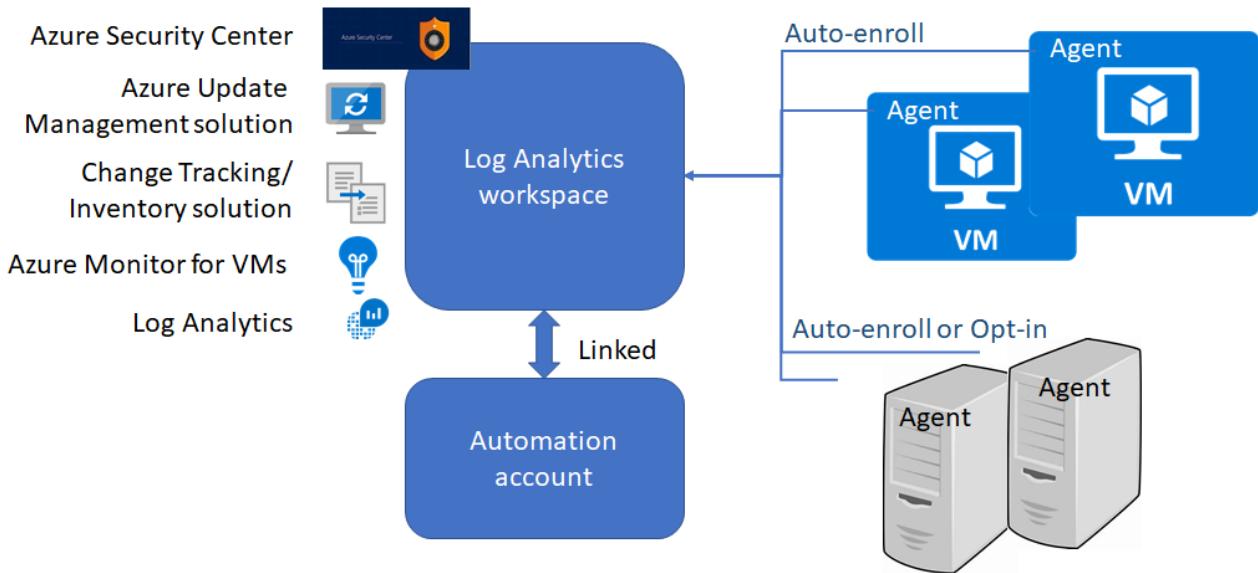
- **Enable management services on a single VM for evaluation by using the portal.** Use this process to familiarize yourself with the Azure server management services.
- **Configure management services for a subscription by using the portal.** This process helps you configure the Azure environment so that any new VMs that are provisioned will automatically use management services. Use this approach if you prefer the Azure portal experience to scripts and command lines.
- **Configure management services for a subscription by using Azure Automation.** This process is fully automated. Just create a subscription, and the scripts will configure the environment to use management services for any newly provisioned VM. Use this approach if you're familiar with PowerShell scripts and Azure Resource Manager templates, or if you want to learn to use them.

The procedures for each of these approaches are different.

## NOTE

When you use the Azure portal, the sequence of onboarding steps differs from the automated onboarding steps. The portal offers a simpler onboarding experience.

The following diagram shows the recommended deployment model for management services:



As shown in the preceding diagram, the Log Analytics agent has two configurations for on-premises servers:

- **Auto-enroll:** When the Log Analytics agent is installed on a server and configured to connect to a workspace, the solutions that are enabled on that workspace are applied to the server automatically.
- **Opt-in:** Even if the agent is installed and connected to the workspace, the solution isn't applied unless it's added to the server's scope configuration in the workspace.

## Next steps

Learn how to onboard a single VM by using the portal to evaluate the onboarding process.

[Onboard a single Azure VM for evaluation](#)

# Enable server management services on a single VM for evaluation

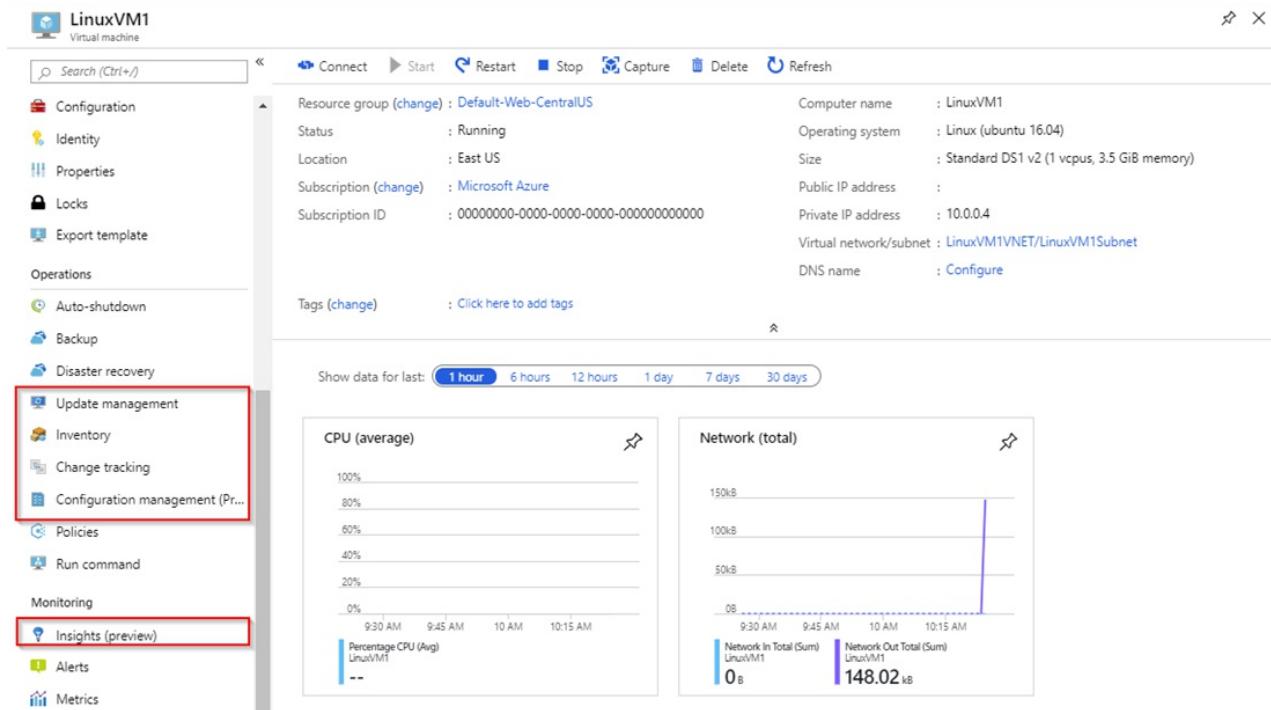
11/9/2020 • 2 minutes to read • [Edit Online](#)

Learn how to enable server management services on a single VM for evaluation.

## NOTE

Create the required [Log Analytics workspace](#) and [Azure Automation account](#) before you implement Azure management services on a VM.

It's simple to onboard Azure server management services to individual virtual machines in the Azure portal. You can familiarize yourself with these services before you onboard them. When you select a VM instance, all the solutions on the list of [management tools and services](#) appear on the **Operations** or **Monitoring** menu. You select a solution and follow the wizard to onboard it.



## Related resources

For more information about how to onboard these solutions to individual VMs, see:

- [Onboard Update Management, Change Tracking, and Inventory solutions from Azure virtual machine](#)
- [Onboard Azure Monitoring for VMs](#)

## Next steps

Learn how to use Azure Policy to onboard Azure VMs at scale.

[Configure Azure management services for a subscription](#)

# Configure Azure server management services at scale

11/9/2020 • 7 minutes to read • [Edit Online](#)

You must complete these two tasks to onboard Azure server management services to your servers:

- Deploy service agents to your servers.
- Enable the management solutions.

This article covers the three processes that are necessary to complete these tasks:

1. Deploy the required agents to Azure VMs by using Azure Policy.
2. Deploy the required agents to on-premises servers.
3. Enable and configuring the solutions.

## NOTE

Create the required [Log Analytics workspace](#) and [Azure Automation account](#) before you onboard virtual machines to Azure server management services.

## Use Azure Policy to deploy extensions to Azure VMs

All the management solutions that are discussed in [Azure management tools and services](#) require that the Log Analytics agent is installed on Azure virtual machines and on-premises servers. You can onboard your Azure VMs at scale by using Azure Policy. Assign policy to ensure that the agent is installed on your Azure VMs and connected to the correct Log Analytics workspace.

Azure Policy has a [built-in policy initiative](#) that includes the Log Analytics Agent and the [Microsoft Dependency Agent](#), which is required by Azure Monitor for VMs.

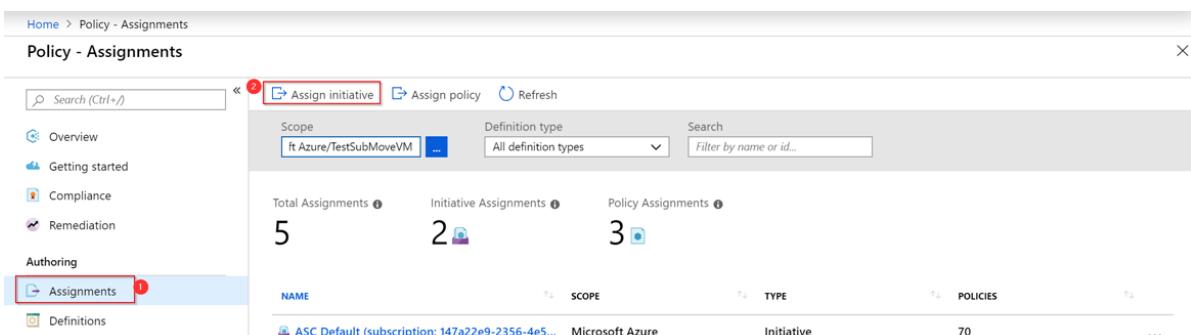
## NOTE

For more information about various agents for Azure monitoring, see [Overview of the Azure monitoring agents](#).

## Assign policies

To assign the policies that described in the previous section:

1. In the Azure portal, go to **Policy > Assignments > Assign initiative**.



The screenshot shows the Azure Policy - Assignments interface. At the top, there's a search bar and buttons for 'Assign initiative', 'Assign policy', and 'Refresh'. Below that, a scope dropdown is set to 'ft Azure/TestSubMoveVM'. The main area displays three counts: Total Assignments (5), Initiative Assignments (2), and Policy Assignments (3). A table below lists one assignment entry:

NAME	SCOPE	TYPE	POLICIES
ASC Default (subscription: 147a22e9-2356-4e5...)	Microsoft Azure	Initiative	70

2. On the **Assign policy** page, set the **Scope** by selecting the ellipsis (...) and then selecting either a

management group or subscription. Optionally, select a resource group. Then choose **Select** at the bottom of the **Scope** page. The scope determines which resources or group of resources the policy is assigned to.

3. Select the ellipsis (...) next to **Policy definition** to open the list of available definitions. To filter the initiative definitions, enter **Azure Monitor** in the **Search** box:

[Preview]: **Enable Azure Monitor for VMs**  
Built-in  
Enable Azure Monitor for the Virtual Machines (VMs) in the specified scope (Management group, Subscription or resource group). Takes Log Analytics workspace as parameter.

4. The **Assignment name** is automatically populated with the policy name that you selected, but you can change it. You can also add an optional description to provide more information about this policy assignment. The **Assigned by** field is automatically filled based on who is signed in. This field is optional, and it supports custom values.
5. For this policy, select **Log Analytics workspace** for the Log analytics agent to associate.

#### PARAMETERS

\* **Log Analytics workspace**  ⓘ  
Click '...' to change the subscription for the parameter. ...

6. Select the **Managed Identity location** check box. If this policy is of the type **DeployIfNotExists**, a managed identity will be required to deploy the policy. In the portal, the account will be created as indicated by the check box selection.
7. Select **Assign**.

After you complete the wizard, the policy assignment will be deployed to the environment. It can take up to 30 minutes for the policy to take effect. To test it, create new VMs after 30 minutes, and check if the Microsoft Monitoring Agent is enabled on the VM by default.

## Install agents on on-premises servers

#### NOTE

Create the required [Log Analytics workspace](#) and [Azure Automation account](#) before you onboard Azure server management services to servers.

For on-premises servers, you need to download and install the [Log Analytics Agent](#) and the [Microsoft Dependency Agent](#) manually and configure them to connect to the correct workspace. You must specify the workspace ID and key information. To get that information, go to your Log Analytics workspace in the Azure portal, then select **Settings > Advanced settings**.

Home > Log Analytics workspaces > ContosoFinanceLogs > Advanced settings

### Advanced settings

contosofinancelogs

Refresh Logs

Connected Sources >	Windows Servers >	Windows Servers Attach any Windows server or client.
Data >	Linux Servers >	<b>0 WINDOWS COMPUTERS CONNECTED</b>
Computer Groups >	Azure Storage >	<a href="#">Download Windows Agent (64 bit)</a>
	System Center >	<a href="#">Download Windows Agent (32 bit)</a>
<p>You'll need the Workspace ID and Key to install the agent.</p> <div style="border: 1px solid red; padding: 5px;"> <p><b>WORKSPACE ID</b> 209f0c715-1255-425d-b0cf-19e085e722924</p> <p><b>PRIMARY KEY</b> apjLmLqyU8VCHtYKZDzmfJ8jy8pPUpeTUQ=</p> <p><a href="#">Regenerate</a></p> <p><b>SECONDARY KEY</b> 209f0c715-1255-425d-b0cf-19e085e722924</p> <p><a href="#">Regenerate</a></p> <p><b>OMS Gateway</b> If you have machines with no internet connectivity to OMS, download the OMS Gateway to act as a proxy. <a href="#">Learn more</a>.</p> <p><a href="#">Download OMS Gateway</a></p> </div>		

## Enable and configure solutions

To enable solutions, you need to configure the Log Analytics workspace. Onboarded Azure VMs and on-premises servers will get the solutions from the Log Analytics workspaces that they're connected to.

### Update Management

The Update Management, Change Tracking, and Inventory solutions require both a Log Analytics workspace and an Automation account. To ensure that these resources are properly configured, we recommend that you onboard through your Automation account. For more information, see [Onboard Update Management, Change Tracking, and Inventory solutions](#).

We recommend that you enable the Update Management solution for all servers. Update Management is free for Azure VMs and on-premises servers. If you enable Update Management through your Automation account, a [scope configuration](#) is created in the workspace. Manually update the scope to include machines that are covered by the Update Management service.

To cover your existing servers as well as future servers, you need to remove the scope configuration. To do this, view your Automation account in the Azure portal. Select **Update Management > Manage machine > Enable on all available and future machines**. This setting allows all Azure VMs that are connected to the workspace to use Update Management.

Home > All resources > AAcountUY1 - Update management

**AAcountUY1 - Update management**  
Automation Account

Search (Ctrl+ /) < Schedule update deployment + Add Azure VMs  Add non-Azure machine

Change tracking State configuration (DSC)

Update management Update management

Non-compliant machines  0 out of 0	Machines need attention (0)	Missing updates (0)
Critical and security 0	Critical 0	Security 0
Other 0	Others 0	
Not assessed 0		

Machines (0) Missing updates (0) Update deployments Scheduled update deployments

**Manage Machines**  
Update Management

These machines are reporting to the Log Analytics workspace 'Update Management' enabled on them. It can take up to available for machines that you enable with this feature.

Enable on all available machines  Enable on all available and future machines  Enable on selected machines

With this option, all current and future machines th

### Change Tracking and Inventory solutions

To onboard the Change Tracking and Inventory solutions, follow the same steps as for Update Management. For

more information about how to onboard these solutions from your Automation account, see [Onboard Update Management, Change Tracking, and Inventory solutions](#).

The Change Tracking solution is free for Azure VMs and costs \$6 per node per month for on-premises servers. This cost covers Change Tracking, Inventory, and Desired State Configuration. If you want to enroll only specific on-premises servers, you can opt in those servers. We recommend that you onboard all your production servers.

#### Opt in via the Azure portal

1. Go to the Automation account that has Change Tracking and Inventory enabled.
2. Select **Change tracking**.
3. Select **Manage machines** in the upper-right pane.
4. Select **Enable on selected machines**. Then select **Add** next to the machine name.
5. Select **Enable** to enable the solution for those machines.

The screenshot shows the 'Change tracking' blade in the Azure portal. On the left, there's a sidebar with various navigation options like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Configuration Management, Inventory, Change tracking (which is selected and highlighted in blue), State configuration (DSC), Update management, and Runbooks. The main area has tabs for Overview, Activity log, and Change tracking. Under Change tracking, there are sections for Change Types (Events, Daemons, Files, Registry, Software, Windows Services) and a summary table showing 'No changes detected'. Below this is a 'Changes (0)' section with a search bar and a table for RESOURCE NAME and CHANGE TYPE. To the right, there's a 'Manage Machines' blade titled 'Change Tracking and Inventory'. It lists '2 machines do not have "Change Tracking and Inventory" enabled'. A section for 'AVAILABLE MACHINES' shows 'testvm' and 'testwin' with 'add' buttons. The 'SELECTED MACHINES' section shows 'testwin' with a 'remove' button. At the bottom, there are 'Enable' and 'Cancel' buttons, with 'Enable' also highlighted with a red box.

#### Opt in by using saved searches

Alternatively, you can configure the scope configuration to opt in on-premises servers. Scope configuration uses saved searches.

To create or modify the saved search, follow these steps:

1. Go to the Log Analytics workspace that is linked to the Automation account that you configured in the preceding steps.
2. Under **General**, select **Saved searches**.
3. In the **Filter** box, enter **Change Tracking** to filter the list of saved searches. In the results, select **MicrosoftDefaultComputerGroup**.
4. Enter the computer name or the VMUUID to include the computers that you want to opt in for Change Tracking.

```
Heartbeat
| where AzureEnvironment=~"Azure" or Computer in~ ("list of the on-premises server names", "server1")
| distinct Computer
```

#### **NOTE**

The server name must exactly match the value in the expression, and it shouldn't contain a domain name suffix.

1. Select **Save**. By default, the scope configuration is linked to the **MicrosoftDefaultComputerGroup** saved search. It will be automatically updated.

### **Azure Activity Log**

[Azure Activity Log](#) is also part of Azure Monitor. It provides insight into subscription-level events that occur in Azure.

To implement this solution:

1. In the Azure portal, open **All services**, then select **Management + Governance > Solutions**.
2. In the **Solutions** view, select **Add**.
3. Search for **Activity Log Analytics** and select it.
4. Select **Create**.

You need to specify the **Workspace name** of the workspace that you created in the previous section where the solution is enabled.

### **Azure Log Analytics Agent Health**

The Azure Log Analytics Agent Health solution reports on the health, performance, and availability of your Windows and Linux servers.

To implement this solution:

1. In the Azure portal, open **All services**, then select **Management + Governance > Solutions**.
2. In the **Solutions** view, select **Add**.
3. Search for **Azure Log Analytics agent health** and select it.
4. Select **Create**.

You need to specify the **Workspace name** of the workspace that you created in the previous section where the solution is enabled.

After creation is complete, the workspace resource instance displays **AgentHealthAssessment** when you select **View > Solutions**.

### **Antimalware Assessment**

The Antimalware Assessment solution helps you identify servers that are infected or at increased risk of infection by malware.

To implement this solution:

1. In the Azure portal, open **All services**, select **select Management + Governance > Solutions**.
2. In the **Solutions** view, select **Add**.
3. Search for and then select **Antimalware Assessment**.
4. Select **Create**.

You need to specify the **Workspace name** of the workspace that you created in the previous section where the solution is enabled.

After creation is complete, the workspace resource instance displays **AntiMalware** when you select **View > Solutions**.

### **Azure Monitor for VMs**

You can enable [Azure Monitor for VMs](#) through the view page for the VM instance, as described in [Enable management services on a single VM for evaluation](#). You shouldn't enable solutions directly from the [Solutions](#) page as you do for the other solutions that are described in this article. For large-scale deployments, it may be easier to use [automation](#) to enable the correct solutions in the workspace.

## Azure Security Center

We recommend that you onboard all your servers at least to the Free tier of Azure Security Center. This option provides basic security assessments and actionable security recommendations for your environment. The Standard tier provides additional benefits. For more information, see [Azure Security Center pricing](#).

To enable the Free tier of Azure Security Center, follow these steps:

1. Go to the [Security Center](#) portal page.
2. Under **POLICY & COMPLIANCE**, select **Security policy**.
3. Find the Log Analytics workspace resource that you created in the pane on the right side.
4. Select **Edit settings** for that workspace.
5. Select **Pricing tier**.
6. Choose the **Free** option.
7. Select **Save**.

## Next steps

Learn how to use automation to onboard servers and create alerts.

[Automate onboarding and alert configuration](#)

# Automate onboarding

11/9/2020 • 2 minutes to read • [Edit Online](#)

To improve the efficiency of deploying Azure server management services, consider automating deployment as discussed in previous sections of this guidance. The script and the example templates provided in the following sections are starting points for developing your own automation of onboarding processes.

This guidance has a supporting GitHub repository of sample code, [CloudAdoptionFramework](#). The repository provides example scripts and Azure Resource Manager templates to help you automate the deployment of Azure server management services.

The sample files illustrate how to use Azure PowerShell cmdlets to automate the following tasks:

- Create a [Log Analytics workspace](#). (Or, use an existing workspace if it meets the requirements. For details, see [Workspace planning](#).)
- Create an Automation account, or use an existing account that meets the requirements. For more information, see [Workspace planning](#).
- Link the Automation account and the Log Analytics workspace. This step isn't required if you're onboarding by using the Azure portal.
- Enable Update Management, and Change Tracking and Inventory, for the workspace.
- Onboard Azure VMs by using Azure Policy. A policy installs the Log Analytics agent and the Microsoft Dependency Agent on the Azure VMs.
- Auto-enable Azure backup for VMs using [Azure Policy](#)
- Onboard on-premises servers by installing the Log Analytics agent on them.

The files described in the following table are used in this sample. You can customize them to support your own deployment scenarios.

FILE NAME	DESCRIPTION
New-AMSDeployment.ps1	The main, orchestrating script that automates onboarding. It creates resource groups, and location, workspace, and Automation accounts, if they don't exist already. This PowerShell script requires an existing subscription.
Workspace-AutomationAccount.json	A Resource Manager template that deploys the workspace and Automation account resources.
WorkspaceSolutions.json	A Resource Manager template that enables the solutions you want in the Log Analytics workspace.
ScopeConfig.json	A Resource Manager template that uses the opt-in model for on-premises servers with the Change Tracking solution. Using the opt-in model is optional.
Enable-VMInsightsPerfCounters.ps1	A PowerShell script that enables VM Insights for servers and configures performance counters.

FILE NAME	DESCRIPTION
ChangeTracking-FileList.json	A Resource Manager template that defines the list of files that will be monitored by Change Tracking.

Use the following command to run `New-AMSDeployment.ps1`:

```
.\New-AMSDeployment.ps1 -SubscriptionName '{Subscription Name}' -WorkspaceName '{Workspace Name}' -  
WorkspaceLocation '{Azure Location}' -AutomationAccountName {Account Name} -AutomationAccountLocation {Account  
Location}
```

## Next steps

Learn how to set up basic alerts to notify your team of key management events and issues.

[Set up basic alerts](#)

# Set up basic alerts

11/9/2020 • 2 minutes to read • [Edit Online](#)

A key part of managing resources is getting notified when problems occur. Alerts proactively notify you of critical conditions, based on triggers from metrics, logs, or service-health issues. As part of onboarding the Azure server management services, you can set up alerts and notifications that help keep your IT teams aware of any problems.

## Azure Monitor alerts

Azure Monitor offers [alerting](#) capabilities to notify you, via email or messaging, when things go wrong. These capabilities are based on a common data-monitoring platform that includes logs and metrics generated by your servers and other resources. By using a common set of tools in Azure Monitor, you can analyze data that's combined from multiple resources and use it to trigger alerts. These triggers can include:

- Metric values.
- Log search queries.
- Activity log events.
- The health of the underlying Azure platform.
- Tests for website availability.

See the [list of Azure Monitor data sources](#) for a more detailed description of the sources of monitoring data that this service collects.

For details about manually creating and managing alerts by using the Azure portal, see the [Azure Monitor documentation](#).

## Automated deployment of recommended alerts

In this guide, we recommend that you create a set of 15 alerts for basic infrastructure monitoring. Find the deployment scripts in the [Azure Alert Toolkit GitHub repository](#).

This package creates alerts for:

- Low disk space
- Low available memory
- High CPU use
- Unexpected shutdowns
- Corrupted file systems
- Common hardware failures

The package uses HP server hardware as an example. Change the settings in the associated configuration file to reflect your OEM hardware. You can also add more performance counters to the configuration file. To deploy the package, run the New-CoreAlerts.ps1 file.

## Next steps

Learn about operations and security mechanisms that support your ongoing operations.

[Ongoing management and security](#)

# Phase 3: Ongoing management and security

11/9/2020 • 2 minutes to read • [Edit Online](#)

After you've onboarded Azure server management services, you'll need to focus on the operations and security configurations that will support your ongoing operations. We'll start with securing your environment by reviewing the Azure Security Center. We'll then configure policies to keep your servers in compliance and automate common tasks. This section covers the following topics:

- [Address security recommendations](#). Azure Security Center provides suggestions to improve the security of your environment. When you implement these recommendations, you see the impact reflected in a security score.
- [Enable the Guest Configuration policy](#). Use the Azure Policy Guest Configuration feature to audit the settings in a virtual machine. For example, you can check whether any certificates are about to expire.
- [Track and alert on critical changes](#). When you're troubleshooting, the first question to consider is, "What's changed?" In this article, you'll learn how to track changes and create alerts to proactively monitor critical components.
- [Create update schedules](#). Schedule the installation of updates to ensure that all your servers have the latest ones.
- [Common Azure Policy examples](#). This article provides examples of common management policies.

## Address security recommendations

Azure Security Center is the central place to manage security for your environment. You'll see an overall assessment and targeted recommendations.

We recommend that you review and implement the recommendations provided by this service. For information about additional benefits of Azure Security Center, see [Follow Azure Security Center recommendations](#).

## Next steps

Learn how to [enable the Azure Policy Guest Configuration feature](#).

[Guest Configuration policy](#)

# Guest Configuration policy

11/9/2020 • 2 minutes to read • [Edit Online](#)

You can use the Azure Policy [Guest Configuration](#) extension to audit the configuration settings in a virtual machine. Guest Configuration is currently supported only on Azure VMs.

To find the list of Guest Configuration policies, search for "Guest Configuration" on the Azure Policy portal page. Or run this cmdlet in a PowerShell window to find the list:

```
Get-AzPolicySetDefinition | where-object {$_.Properties.metadata.category -eq "Guest Configuration"}
```

## NOTE

Guest Configuration functionality is regularly updated to support additional policy sets. Check for new supported policies periodically and evaluate whether they'll be useful.

## Deployment

Use the following example PowerShell script to deploy these policies to:

- Verify that password security settings in Windows and Linux computers are set correctly.
- Verify that certificates aren't close to expiration on Windows VMs.

Before you run this script, use the [Connect-AzAccount](#) cmdlet to sign in. When you run the script, you must provide the name of the subscription that you want to apply the policies to.

```
# Assign Guest Configuration policy.

param (
    [Parameter(Mandatory=$true)]
    [string] $SubscriptionName
)

$Subscription = Get-AzSubscription -SubscriptionName $SubscriptionName
$scope = "/subscriptions/" + $Subscription.Id

$PasswordPolicy = Get-AzPolicySetDefinition -Name "3fa7cbf5-c0a4-4a59-85a5-cca4d996d5a6"
$CertExpirePolicy = Get-AzPolicySetDefinition -Name "b6f5e05c-0aaa-4337-8dd4-357c399d12ae"

New-AzPolicyAssignment -Name "PasswordPolicy" -DisplayName "[Preview]: Audit that password security
settings are set correctly inside Linux and Windows machines" -Scope $scope -PolicySetDefinition
$PasswordPolicy -AssignIdentity -Location eastus

New-AzPolicyAssignment -Name "CertExpirePolicy" -DisplayName "[Preview]: Audit that certificates are not
expiring on Windows VMs" -Scope $scope -PolicySetDefinition $CertExpirePolicy -AssignIdentity -Location eastus
```

## Next steps

Learn how to [enable change tracking and alerting](#) for critical file, service, software, and registry changes.

[Enable tracking and alerting for critical changes](#)

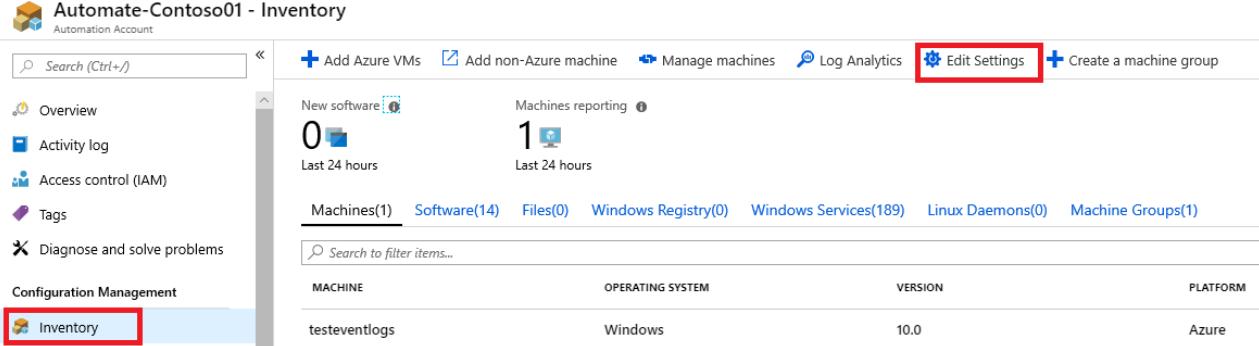


# Enable tracking and alerting for critical changes

11/9/2020 • 3 minutes to read • [Edit Online](#)

Azure Change Tracking and Inventory provide alerts on the configuration state of your hybrid environment and changes to that environment. It can report critical file, service, software, and registry changes that might affect your deployed servers.

By default, the Azure Automation inventory service doesn't monitor files or registry settings. The solution does provide a list of registry keys that we recommend for monitoring. To see this list, go to your Automation account in the Azure portal, then select **Inventory > Edit settings**.



The screenshot shows the Azure Automation - Contoso01 - Inventory page. On the left, there's a sidebar with links like Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Configuration Management, and Inventory (which is highlighted with a red box). At the top, there are buttons for Add Azure VMs, Add non-Azure machine, Manage machines, Log Analytics, Edit Settings (which is highlighted with a red box), and Create a machine group. Below these, there are sections for New software (0 last 24 hours) and Machines reporting (1 last 24 hours). A table lists Machines (1), Software (14), Files (0), Windows Registry (0), Windows Services (189), Linux Daemons (0), and Machine Groups (1). A search bar is at the bottom of the table. The main content area shows a single machine entry: testeventlogs, Windows operating system, version 10.0, and platform Azure.

For more information about each registry key, see [Registry key change tracking](#). Select any key to evaluate and then enable it. The setting is applied to all VMs that are enabled in the current workspace.

You can also use the service to track critical file changes. For example, you might want to track the C:\windows\system32\drivers\etc\hosts file because the OS uses it to map host names to IP addresses. Changes to this file could cause connectivity problems or redirect traffic to dangerous websites.

To enable file-content tracking for the hosts file, follow the steps in [Enable file content tracking](#).

You can also add an alert for changes to files that you're tracking. For example, say you want to set an alert for changes to the hosts file. Select **Log Analytics** on the command bar or Log Search for the linked Log Analytics workspace. In Log Analytics, use the following query to search for changes to the hosts file:

```
ConfigurationChange | where FieldsChanged contains "FileContentChecksum" and FileSystemPath contains "hosts"
```



The screenshot shows the Log Analytics workspace. At the top, there are buttons for Run, Save, Copy link, Export, New alert rule, and Pin. The time range is set to Last 24 hours. Below the buttons, the query is displayed: ConfigurationChange | where FieldsChanged contains "FileContentChecksum" and FileSystemPath contains "hosts". The results table is empty, indicating no recent changes.

This query searches for changes to the contents of files that have a path that contains the word "hosts." You can also search for a specific file by changing the path parameter. (For example,

```
FileSystemPath == "c:\\windows\\system32\\drivers\\etc\\hosts" .)
```

After the query returns the results, select **New alert rule** to open the alert-rule editor. You can also get to this editor via Azure Monitor in the Azure portal.

In the alert-rule editor, review the query and change the alert logic if you need to. In this case, we want the alert to be raised if any changes are detected on any machine in the environment.

**\* Search query**

```
ConfigurationChange | where FieldsChanged contains "FileContentChecksum" and FileSystemPath contains "hosts"
```

Query to be executed : ConfigurationChange | where FieldsChanged contains "FileContentChecksum" and FileSystemPath contains "hosts" &| count  
For time window : 1/4/2019, 4:17:49 PM - 1/4/2019, 4:22:49 PM

**Alert logic**

Based on	Condition	* Threshold
Number of results	Greater than	1

**Condition preview**

Whenever the custom log search is greater than 1 count

**Evaluated based on**

* Period (in minutes)	* Frequency (in minutes)
5	5

After you set the condition logic, you can assign action groups to perform actions in response to the alert. In this example, when the alert is raised, emails are sent and an ITSM ticket is created. You can take many other useful actions, like triggering an Azure function, an Azure Automation runbook, a webhook, or a logic app.

**RESOURCE**  
contosomarketingworkspace  
[Select](#)

**HIERARCHY**  
Contoso IT - demo > contosoautomation

**CONDITION**  
Whenever the Custom log search is Greater than 1 count  
Monthly cost in USD (Estimated) \$ 1.50  
Total \$ 1.50  
[Add condition](#)

**ACTION GROUPS**  
Notify your team via email and text messages or automate actions using webhooks, runbooks, functions, logic apps or integrating with external ITSM solutions. Learn more [here](#)

ACTION GROUP NAME	ACTION GROUP TYPE
Create Ticket	1 ITSM
Send Email	2 Email(s)

[Select existing](#) [Create New](#)

After you've set all the parameters and logic, apply the alert to the environment.

## Tracking and alerting examples

This section shows other common scenarios for tracking and alerting that you might want to use.

### Driver file changed

Use the following query to detect if driver files are changed, added, or removed. It's useful for tracking changes to critical system files.

```
ConfigurationChange | where ConfigChangeType == "Files" and FileSystemPath contains "c:\\windows\\system32\\drivers\\\"
```

## Specific service stopped

Use the following query to track changes to system-critical services.

```
ConfigurationChange | where SvcState == "Stopped" and SvcName contains "w3svc"
```

## New software installed

Use the following query for environments that need to lock down software configurations.

```
ConfigurationChange | where ConfigChangeType == "Software" and ChangeCategory == "Added"
```

## Specific software version is or isn't installed on a machine

Use the following query to assess security. This query references `ConfigurationData`, which contains the logs for inventory and provides the last-reported configuration state, not changes.

```
ConfigurationData | where SoftwareName contains "Monitoring Agent" and CurrentVersion != "8.0.11081.0"
```

## Known DLL changed through the registry

Use the following query to detect changes to well-known registry keys.

```
ConfigurationChange | where RegistryKey == "HKEY_LOCAL_MACHINE\\System\\CurrentControlSet\\Control\\Session Manager\\KnownDlls"
```

## Next steps

Learn how Azure Automation can [create update schedules](#) to manage updates for your servers.

[Create update schedules](#)

# Create update schedules

11/9/2020 • 2 minutes to read • [Edit Online](#)

You can manage update schedules by using the Azure portal or the new PowerShell cmdlet modules.

To create an update schedule via the Azure portal, see [Schedule an update deployment](#).

The `Az.Automation` module now supports configuring update management by using Azure PowerShell. [Version 1.7.0](#) of the module adds support for the `New-AzAutomationUpdateManagementAzureQuery` cmdlet. This cmdlet lets you use tags, location, and saved searches to configure update schedules for a flexible group of machines.

## Example script

The example script in this section illustrates the use of tagging and querying to create dynamic groups of machines that you can apply update schedules to. It performs the following actions. You can refer to the implementations of the specific actions when you create your own scripts.

- Creates an Azure Automation update schedule that runs every Saturday at 8:00 AM.
- Creates a query for any machines that match these criteria:
  - Deployed in the `westus`, `eastus`, or `eastus2` Azure location.
  - Has an `Owner` tag applied with a value set to `JaneSmith`.
  - Has a `Production` tag applied with a value set to `true`.
- Applies the update schedule to the queried machines and sets a two-hour update window.

Before you run the example script, you'll need to sign in by using the `Connect-AzAccount` cmdlet. When you start the script, provide the following information:

- The target subscription ID
- The target resource group
- Your Log Analytics workspace name
- Your Azure Automation account name

```

<#
    .SYNOPSIS
        This script orchestrates the deployment of the solutions and the agents.
    .Parameter SubscriptionName
    .Parameter WorkspaceName
    .Parameter AutomationAccountName
    .Parameter ResourceGroupName

#>

param (
    [Parameter(Mandatory=$true)]
    [string] $SubscriptionId,
    [Parameter(Mandatory=$true)]
    [string] $ResourceGroupName,
    [Parameter(Mandatory=$true)]
    [string] $WorkspaceName,
    [Parameter(Mandatory=$true)]
    [string] $AutomationAccountName,
    [Parameter(Mandatory=$false)]
    [string] $scheduleName = "SaturdayCriticalSecurity"
)

Import-Module Az.Automation

$startTime = ([DateTime]::Now).AddMinutes(10)
$schedule = New-AzAutomationSchedule -ResourceGroupName $ResourceGroupName `

    -AutomationAccountName $AutomationAccountName `

    -StartTime $startTime `

    -Name $scheduleName `

    -Description "Saturday patches" `

    -DaysOfWeek Saturday `

    -WeekInterval 1 `

    -ForUpdateConfiguration

# Using AzAutomationUpdateManagementAzureQuery to create dynamic groups.

$queryScope = @("/subscriptions/$SubscriptionID/resourceGroups/")

$query1Location =@("westus", "eastus", "eastus2")
$query1FilterOperator = "Any"
$ownerTag = @{ "Owner"= @("JaneSmith") }
$ownerTag.Add("Production", "true")

$DGQuery = New-AzAutomationUpdateManagementAzureQuery -ResourceGroupName $ResourceGroupName `

    -AutomationAccountName $AutomationAccountName `

    -Scope $queryScope `

    -Tag $ownerTag

$AzureQueries = @($DGQuery)

$updateConfig = New-AzAutomationSoftwareUpdateConfiguration -ResourceGroupName $ResourceGroupName `

    -AutomationAccountName $AutomationAccountName `

    -Schedule $schedule `

    -Windows `

    -Duration (New-TimeSpan -Hours 2) `

    -AzureQuery $AzureQueries `

    -IncludedUpdateClassification Security,Critical

```

## Next steps

See examples of how to implement [common policies in Azure](#) that can help manage your servers.

[Common policies in Azure](#)

# Common Azure Policy examples

11/9/2020 • 2 minutes to read • [Edit Online](#)

Azure Policy can help you apply governance to your cloud resources. This service can help you create guardrails that ensure company-wide compliance to governance policy requirements. To create policies, use either the Azure portal or PowerShell cmdlets. This article provides PowerShell cmdlet examples.

## NOTE

With Azure Policy, enforcement policies (`DeployIfNotExists`) aren't automatically deployed to existing VMs. Remediation is required to keep VMs in compliance. For more information, see [Remediate noncompliant resources with Azure Policy](#).

## Common policy examples

The following sections describe some commonly used policies.

### Restrict resource regions

Regulatory and policy compliance often depends on control of the physical location where resources are deployed. You can use a built-in policy to allow users to create resources only in certain allowed Azure regions.

To find this policy in the portal, search for "location" on the policy definition page. Or run this cmdlet to find the policy:

```
Get-AzPolicyDefinition | Where-Object { ($_.Properties.policyType -eq 'BuiltIn') `  
-and ($_.Properties.displayName -like '*location*') }
```

The following script shows how to assign the policy. Change the `$subscriptionID` value to point to the subscription that you want to assign the policy to. Before you run the script, use the [Connect-AzAccount](#) cmdlet to sign in.

```
# Specify the value for $SubscriptionID.  
$SubscriptionID = <subscription ID>  
$scope = "/subscriptions/$SubscriptionID"  
  
# Replace the -Name GUID with the policy GUID you want to assign.  
$AllowedLocationPolicy = Get-AzPolicyDefinition -Name "e56962a6-4747-49cd-b67b-bf8b01975c4c"  
  
# Replace the locations with the ones you want to specify.  
$policyParam = '{ "listOfAllowedLocations":{ "value":["eastus","westus"]}}'  
New-AzPolicyAssignment -Name "Allowed Location" -DisplayName "Allowed locations for resource creation" -Scope  
$scope -PolicyDefinition $AllowedLocationPolicy -Location eastus -PolicyParameter $policyParam
```

You can also use this script to apply the other policies that are discussed in this article. Just replace the GUID in the line that sets `$AllowedLocationPolicy` with the GUID of the policy that you want to apply.

### Block certain resource types

Another common built-in policy that's used to control costs can also be used to block certain resource types.

To find this policy in the portal, search for "allowed resource types" on the policy definition page. Or run this cmdlet to find the policy:

```
Get-AzPolicyDefinition | Where-Object { ($_.Properties.policyType -eq "BuiltIn") -and  
($_.Properties.displayName -like "*allowed resource types") }
```

After you identify the policy that you want to use, you can modify the PowerShell sample in the [Restrict resource regions](#) section to assign the policy.

## Restrict VM size

Azure offers a wide range of VM sizes to support various workloads. To control your budget, you could create a policy that allows only a subset of VM sizes in your subscriptions.

## Deploy antimalware

You can use this policy to deploy a Microsoft Antimalware extension with a default configuration to VMs that aren't protected by antimalware.

The policy GUID is `2835b622-407b-4114-9198-6f7064cbe0dc`.

The following script shows how to assign the policy. To use the script, change the `$SubscriptionID` value to point to the subscription that you want to assign the policy to. Before you run the script, use the [Connect-AzAccount](#) cmdlet to sign in.

```
# Specify the value for $SubscriptionID.  
$subscriptionID = <subscription ID>  
$scope = "/subscriptions/$subscriptionID"  
  
$antimalwarePolicy = Get-AzPolicyDefinition -Name "2835b622-407b-4114-9198-6f7064cbe0dc"  
  
# Replace location "eastus" with the value that you want to use.  
New-AzPolicyAssignment -Name "Deploy Antimalware" -DisplayName "Deploy default Microsoft IaaSAntimalware  
extension for Windows Server" -Scope $scope -PolicyDefinition $antimalwarePolicy -Location eastus -  
AssignIdentity
```

## Next steps

Learn about other server-management tools and services that are available.

[Azure server management tools and services](#)

# Azure server management tools and services

11/9/2020 • 4 minutes to read • [Edit Online](#)

As is discussed in the [overview](#) of this guidance, the suite of Azure server management services covers these areas:

- Migrate
- Secure
- Protect
- Monitor
- Configure
- Govern

The following sections briefly describe these management areas and provide links to detailed content about the main Azure services that support them.

## Migrate

Migration services can help you migrate your workloads into Azure. To provide the best guidance, the Azure Migrate service starts by measuring on-premises server performance and assessing suitability for migration. After Azure Migrate completes the assessment, you can use [Azure Site Recovery](#) and [Azure Database Migration Service](#) to migrate your on-premises machines to Azure.

## Secure

[Azure Security Center](#) is a comprehensive security management application. By onboarding to Security Center, you can quickly get an assessment of the security and regulatory compliance status of your environment. For instructions on onboarding your servers to Azure Security Center, see [Configure Azure management services for a subscription](#).

## Protect

To protect your data, you need to plan for backup, high availability, encryption, authorization, and related operational issues. These topics are covered extensively online, so here we'll focus on building a business continuity and disaster recovery (BCDR) plan. We'll include references to documentation that describes in detail how to implement and deploy this type of plan.

When you build data-protection strategies, first consider breaking down your workload applications into their different tiers. This approach helps because each tier typically requires its own unique protection plan. To learn more about designing applications to be resilient, see [Designing resilient applications for Azure](#).

The most basic data protection is backup. To speed up the recovery process if servers are lost, back up not just data but also server configurations. Backup is an effective mechanism to handle accidental data deletion and ransomware attacks. [Azure Backup](#) can help you protect your data on Azure and on-premises servers running Windows or Linux. For details about what Backup can do and for how-to guides, see the [Azure Backup service overview](#).

If a workload requires real-time business continuity for hardware failures or datacenter outage, consider using data replication. [Azure Site Recovery](#) provides continuous replication of your VMs, a solution that provides bare-minimum data loss. Site Recovery also supports several replication scenarios, such as replication:

- Of Azure VMs between two Azure regions.
- Between servers on-premises.
- Between on-premises servers and Azure.

For more information, see the [complete Azure Site Recovery replication matrix](#).

For your file-server data, another service to consider is [Azure File Sync](#). This service helps you centralize your organization's file shares in Azure Files, while preserving the flexibility, performance, and compatibility of an on-premises file server. To use this service, follow the instructions for deploying Azure File Sync.

## Monitor

[Azure Monitor](#) provides a view into various resources, like applications, containers, and virtual machines. It also collects data from several sources:

- [Azure Monitor for VMs](#) provides an in-depth view of VM health, performance trends, and dependencies. The service monitors the health of the operating systems of your Azure virtual machines, virtual-machine scale sets, and machines in your on-premises environment.
- [Log Analytics](#) is a feature of Azure Monitor. Its role is central to the overall Azure management story. It serves as the data store for log analysis and for many other Azure services. It offers a rich query language and an analytics engine that provides insights into the operation of your applications and resources.
- [Azure Activity Log](#) is also a feature of Azure Monitor. It provides insight into subscription-level events that occur in Azure.

## Configure

Several services fit into this category. They can help you to:

- Automate operational tasks.
- Manage server configurations.
- Measure update compliance.
- Schedule updates.
- Detect changes to your servers.

These services are essential to supporting ongoing operations:

- [Update Management](#) automates the deployment of patches across your environment, including deployment to operating-system instances running outside of Azure. It supports both Windows and Linux operating systems, and tracks key OS vulnerabilities and nonconformance caused by missing patches.
- [Change Tracking and Inventory](#) provides insight into the software that's running in your environment, and highlights any changes that have occurred.
- [Azure Automation](#) lets you run Python and PowerShell scripts or runbooks to automate tasks across your environment. When you use Automation with the [Hybrid Runbook Worker](#), you can extend your runbooks to your on-premises resources as well.
- [Azure Automation State Configuration](#) enables you to push PowerShell Desired State Configuration (DSC) configurations directly from Azure. DSC also lets you monitor and preserve configurations for guest operating systems and workloads.

## Govern

Adopting and moving to the cloud creates new management challenges. It requires a different mindset as you shift from an operational management burden to monitoring and governance. The Cloud Adoption Framework starts with [governance](#). The framework explains how to migrate to the cloud, what the journey will look like, and who should be involved.

The governance design for standard organizations often differs from governance design for complex enterprises. To learn more about governance best practices for a standard organization, see the [standard enterprise governance guide](#). To learn more about governance best practices for a complex enterprise, see the [governance guide for complex enterprises](#).

## Billing information

To learn about pricing for Azure management services, go to these pages:

- [Azure Site Recovery](#)
- [Azure Backup](#)
- [Azure Monitor](#)
- [Azure Security Center](#)
- [Azure Automation](#), including:
  - Desired State Configuration
  - Azure Update Management service
  - Azure Change Tracking and Inventory services
- [Azure Policy](#)
- [Azure File Sync service](#)

### NOTE

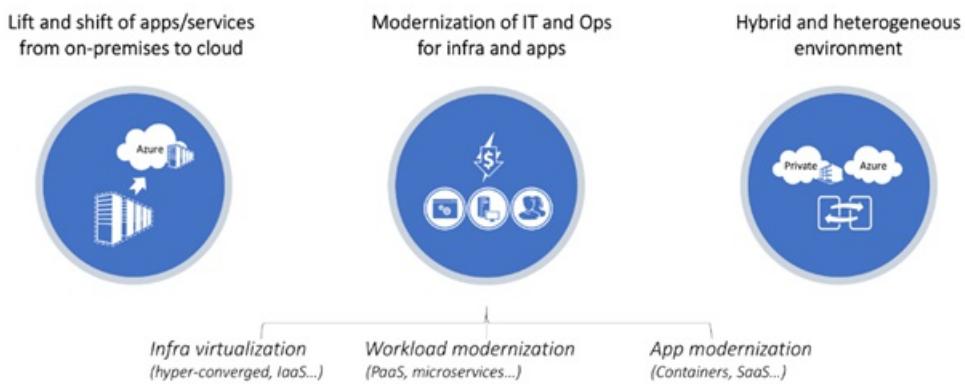
The Azure Update Management solution is free, but there's a small cost related to data ingestion. As a rule of thumb, the first 5 gigabytes (GB) per month of data ingestion are free. We generally observe that each machine uses about 25 MB per month. So, about 200 machines per month are covered for free. For more servers, multiply the number of additional servers by 25 MB per month. Then, multiply the result by the storage price for the additional storage that you need. For information about costs, see [Azure Storage Overview pricing](#). Each additional server typically has a nominal impact on cost.

# Cloud monitoring guide: Introduction

11/9/2020 • 3 minutes to read • [Edit Online](#)

The cloud fundamentally changes how enterprises procure and use technology resources. In the past, enterprises assumed ownership of and responsibility for all levels of technology, from infrastructure to software. Now, the cloud offers the potential for enterprises to provision and consume resources as needed.

Although the cloud offers nearly unlimited flexibility in terms of design choices, enterprises seek proven and consistent methodology for the adoption of cloud technologies. Each enterprise has different goals and timelines for cloud adoption, making a one-size-fits-all approach to adoption nearly impossible.



This digital transformation also enables an opportunity to modernize your infrastructure, workloads, and applications. Depending on business strategy and objectives, adopting a hybrid cloud model is likely part of the migration journey from on-premises to operating fully in the cloud. During this journey, IT teams are challenged to adopt and realize rapid value from the cloud. IT must also understand how to effectively monitor the application or service that's migrating to Azure, and continue to deliver effective IT operations and DevOps.

Stakeholders want to use cloud-based, software as a service (SaaS) monitoring and management tools. They need to understand what services and solutions deliver to achieve end-to-end visibility, reduce costs, and focus less on infrastructure and maintenance of traditional software-based IT operations tools.

However, IT often prefers to use the tools they've already made a significant investment in. This approach supports their service operations processes to monitor both cloud models, with the eventual goal of transitioning to a SaaS-based offering. IT prefers this approach not only because it takes time, planning, resources, and funding to switch. It's also because of confusion about which products or Azure services are appropriate or applicable to achieve the transition.

The goal of this guide is to provide a detailed reference to help enterprise IT managers, business decision makers, application architects, and application developers understand:

- Azure monitoring platforms, with an overview and comparison of their capabilities.
- The best-fit solution for monitoring hybrid, private, and Azure native workloads.
- The recommended end-to-end monitoring approach for both infrastructure and applications. This approach includes deployable solutions for migrating these common workloads to Azure.

This guide isn't a how-to article for using or configuring individual Azure services and solutions, but it does reference those sources when they're applicable or available. After you've read it, you'll understand how to successfully operate a workload by following best practices and patterns.

If you're unfamiliar with Azure Monitor and System Center Operations Manager, and you want to get a better understanding of what makes them unique and how they compare to each other, review the [Overview of our](#)

monitoring platforms.

## Audience

This guide is useful primarily for enterprise administrators, IT operations, IT security and compliance, application architects, workload development owners, and workload operations owners.

## How this guide is structured

This article is part of a series. The following articles are meant to be read together, in order:

- Introduction (this article)
- [Monitoring strategy for cloud deployment models](#)
- [Collect the right data](#)
- [Alerting](#)

## Products and services

A few software and services are available to help you monitor and manage a variety of resources that are hosted in Azure, your corporate network, or other cloud providers. They are:

- [System Center Operations Manager](#)
- [Azure Monitor](#) (includes Log Analytics and Application Insights)
- [Azure Policy](#) and [Azure Blueprints](#)
- [Azure Arc](#)
- [Azure Automation](#)
- [Azure Logic Apps](#)
- [Azure Event Hubs](#)

This first version of the guide covers our current monitoring platforms: Azure Monitor and System Center Operations Manager. It also outlines our recommended strategy for monitoring each of the cloud deployment models. Also included is the first set of monitoring recommendations, starting with data collection and alerting.

## Next steps

[Monitoring strategy for cloud deployment models](#)

# Cloud monitoring guide: Monitoring strategy for cloud deployment models

11/9/2020 • 17 minutes to read • [Edit Online](#)

This article includes our recommended monitoring strategy for each of the cloud deployment models, based on the following criteria:

- You must maintain your commitment to Operations Manager or another enterprise monitoring platform, because it's integrated with your IT operations processes, knowledge, and expertise, or certain functionality isn't available yet in Azure Monitor.
- You must monitor workloads both on-premises and in the public cloud, or just in the cloud.
- Your cloud migration strategy includes modernizing IT operations and moving to our cloud monitoring services and solutions.
- You might have critical systems that are air-gapped or physically isolated, or are hosted in a private cloud or on physical hardware, and these systems need to be monitored.

Our strategy includes support for monitoring infrastructure (compute, storage, and server workloads), application (end-user, exceptions, and client), and network resources. It delivers a complete, service-oriented monitoring perspective.

## Azure cloud monitoring

Azure Monitor is the Azure native platform service that provides a single source for monitoring Azure resources. It's designed for cloud solutions that:

- Are built on Azure.
- Support a business capability that's based on virtual machine (VM) workloads or complex architectures that use microservices and other platform resources.

It monitors all layers of the stack, starting with tenant services, such as Azure Active Directory Domain Services, and subscription-level events and Azure Service Health.

It also monitors infrastructure resources, such as VMs, storage, and network resources. At the top layer, it monitors your application.

By monitoring each of these dependencies, and collecting the right signals that each can emit, you get the observability of applications and the key infrastructure you need.

Our recommended approach to monitoring each layer of the stack is summarized in the following table:

LAYER	RESOURCE	SCOPE	METHOD
Application	A web-based application that runs on .NET, .NET Core, Java, JavaScript, and Node.js platform on an Azure VM, Azure App Service, Azure Service Fabric, Azure Functions, and Azure Cloud Services.	Monitor a live web application to automatically detect performance anomalies, identify code exceptions and issues, and collect user behavior analytics.	Application Insights (a feature of Azure Monitor).

LAYER	RESOURCE	SCOPE	METHOD
Azure resources - platform as a service (PaaS)	Azure Database services (for example, SQL or MySQL).	Azure Database for SQL performance metrics.	Enable diagnostics logging to stream SQL data to Azure Monitor Logs.
Azure resources - infrastructure as a service (IaaS)	1. Azure Storage 2. Azure <a href="#">load balancing services</a> 3. Network security groups 4. Azure Virtual Machines 5. <a href="#">Azure Kubernetes Service/Azure Container Instances</a>	1. Capacity, availability, and performance. 2. Performance and diagnostics logs (activity, access, performance, and firewall). 3. Monitor events when rules are applied, and the rule counter for how many times a rule is applied to deny or allow. 4. Monitor capacity, availability, and performance in a guest VM operating system (OS). Map app dependencies hosted on each VM, including the visibility of active network connections between servers, inbound and outbound connection latency, and ports across any TCP-connected architecture. 5. Monitor capacity, availability, and performance of workloads running on containers and container instances.	For items 1 through 5 in the first column, platform metrics and the Activity log are automatically collected and available in Azure Monitor for analysis and alerting. Configure Diagnostic Settings to forward resource logs to Azure Monitor Logs. 4. Enable <a href="#">Azure Monitor for VMs</a> . 5. Enable <a href="#">Azure Monitor for containers</a> .
Network	Communication between your virtual machine and one or more endpoints (another VM, a fully qualified domain name, a uniform resource identifier, or an IPv4 address).	Monitor reachability, latency, and network topology changes that occur between the VM and the endpoint.	Azure Network Watcher.

LAYER	RESOURCE	SCOPE	METHOD
Azure subscription	Azure Service Health and basic resource health from the perspective of the Azure service.	<ul style="list-style-type: none"> <li>Administrative actions performed on a service or resource.</li> <li>Service health of an Azure service is in a degraded or unavailable state.</li> <li>Health issues detected with an Azure resource from the Azure service perspective.</li> <li>Operations performed with Azure Autoscale indicating a failure or exception.</li> <li>Operations performed with Azure Policy indicating that an allowed or denied action occurred.</li> <li>Record of alerts generated by Azure Security Center.</li> </ul>	Delivered in the Activity Log for monitoring and alerting by using Azure Monitor.
Azure tenant	Azure Active Directory	Azure AD audit logs and sign-in logs.	Enable <a href="#">diagnostics logging</a> , and configure streaming to Azure Monitor Logs.

## Hybrid cloud monitoring

For many organizations, transition to the cloud must be approached gradually, where the hybrid cloud model is the most common first step in the journey. You carefully select the appropriate subset of applications and infrastructure to begin your migration, while you avoid disruption to your business. However, because we offer two monitoring platforms that support this cloud model, IT decision makers might be uncertain as to which is the best choice to support their business and IT operational goals.

In this section, we address the uncertainty by reviewing several factors and offering an understanding of which platform to consider.

Keep in mind the following key technical aspects:

- You need to collect data from Azure resources that support the workload, and forward them to your existing on-premises or managed service provider tools.
- You need to maintain your current investment in System Center Operations Manager, and configure it to monitor IaaS and PaaS resources that are running in Azure. Optionally, because you're monitoring two environments with different characteristics, based on your requirements, you need to determine how integrating with Azure Monitor supports your strategy.
- As part of your modernization strategy to standardize on a single tool to reduce cost and complexity, you need to commit to Azure Monitor for monitoring the resources in Azure and on your corporate network.

The following table summarizes the requirements that Azure Monitor and System Center Operations Manager support with monitoring the hybrid cloud model based on a common set of criteria.

REQUIREMENT	AZURE MONITOR	OPERATIONS MANAGER
-------------	---------------	--------------------

Requirement	Azure Monitor	Operations Manager
Infrastructure requirements	No	<p>Yes</p> <p>Requires, at a minimum, a management server and a SQL server to host the operational database and the reporting data warehouse database. The complexity increases when high availability and disaster recovery are required, and there are machines in multiple sites, untrusted systems, and other complex design considerations.</p>
Limited connectivity - no internet or isolated network	No	Yes
Limited connectivity - controlled internet access	Yes	Yes
Limited connectivity - frequently disconnected	Yes	Yes
Configurable health monitoring	No	Yes
Web app availability test (isolated network)	Yes, limited  Azure Monitor has limited support in this area and requires custom firewall exceptions.	Yes
Web app availability test (globally distributed)	No	Yes
Monitor VM workloads	Yes, limited  Can collect IIS and SQL Server error logs, Windows events, and performance counters. Requires creating custom queries, alerts, and visualizations.	<p>Yes</p> <p>Supports monitoring most of the server workloads with available management packs. Requires either the Log Analytics Windows agent or Operations Manager agent on the VM, reporting back to the management group on the corporate network.</p>
Monitor Azure IaaS	Yes	<p>Yes</p> <p>Supports monitoring most of the infrastructure from the corporate network. Tracks availability state, metrics, and alerts for Azure VMs, SQL, and storage via the Azure management pack.</p>
Monitor Azure PaaS	Yes	<p>Yes, limited</p> <p>Based on what's supported in the Azure management pack.</p>

Requirement	Azure Monitor	Operations Manager
Azure service monitoring	Yes	Yes  Although there's no native monitoring of Azure Service Health provided today through a management pack, you can create custom workflows to query Service Health alerts. Use the Azure REST API to get alerts through your existing notifications.
Modern web application monitoring	Yes	No
Legacy web application monitoring	Yes, limited, varies by SDK  Supports monitoring older versions of .NET and Java web applications.	Yes, limited
Monitor Azure Kubernetes Service containers	Yes	No
Monitor Docker or Windows containers	Yes	No
Network performance monitoring	Yes	Yes, limited  Supports availability checks, and collects basic statistics from network devices by using the Simple Network Management Protocol (SNMP) from the corporate network.
Interactive data analysis	Yes	No  Relies on SQL Server Reporting Services canned or custom reports, third-party visualization solutions, or a custom Power BI implementation. There are scale and performance limitations with the Operations Manager data warehouse. Integrate with Azure Monitor Logs as an alternative for data aggregation requirements. You achieve integration by configuring the Log Analytics connector.
End-to-end diagnostics, root-cause analysis, and timely troubleshooting	Yes	Yes, limited  Supports end-to-end diagnostics and troubleshooting only for on-premises infrastructure and applications. Uses other System Center components or partner solutions.
Interactive visualizations (Dashboards)	Yes	Yes, limited  Delivers essential dashboards with its HTML5 web console or an advanced experience from partner solutions, such as Squared Up and Savision.

Requirement	Azure Monitor	Operations Manager
Integration with IT or DevOps tools	Yes	Yes, limited

## Collect and stream monitoring data to third-party or on-premises tools

To collect metrics and logs from Azure infrastructure and platform resources, you need to enable Azure Diagnostics logs for those resources. Additionally, with Azure VMs, you can collect metrics and logs from the guest OS by enabling the Azure Diagnostics extension. To forward the diagnostics data that's emitted from your Azure resources to your on-premises tools or managed service provider, configure [Event Hubs](#) to stream the data to them.

## Monitor with System Center Operations Manager

Although System Center Operations Manager was originally designed as an on-premises solution to monitor across applications, workloads, and infrastructure components that are running in your IT environment, it evolved to include cloud-monitoring capabilities. It integrates with Azure, Microsoft 365, and Amazon Web Services (AWS). It can monitor across these diverse environments with management packs that are designed and updated to support them.

For customers who have made significant investments in Operations Manager to achieve comprehensive monitoring that's tightly integrated with their IT service management processes and tools, or for customers new to Azure, it's understandable to ask the following questions:

- Can Operations Manager continue to deliver value, and does it make business sense?
- Do the features in Operations Manager make it the right fit for our IT organization?
- Does integrating Operations Manager with Azure Monitor provide the cost-effective and comprehensive monitoring solution that we require?

If you've already invested in Operations Manager, you don't need to focus on planning a migration to replace it immediately. With Azure or other cloud providers that exist as an extension of your own on-premises network, Operations Manager can monitor the guest VMs and Azure resources as if they were on your corporate network. This approach requires a reliable network connection between your network and the virtual network in Azure that has sufficient bandwidth.

To monitor the workloads that are running in Azure, you need:

- The [System Center Operations Manager Management Pack for Azure](#). It collects performance metrics emitted by Azure services such as web and worker roles, Application Insights availability tests (web tests), Azure Service Bus, and so on. The management pack uses the Azure REST API to monitor the availability and performance of these resources. Some Azure service types have no metrics or predefined monitors in the Management Pack, but you can still monitor them through the relationships defined in the Azure Management Pack for discovered services.
- The [Management Pack for Azure SQL Database](#) to monitor the availability and performance of Azure SQL databases and Azure SQL database servers using the Azure REST API and T-SQL queries to SQL Server system views.
- To monitor the guest OS and workloads that are running on the VM, such as SQL Server, IIS, or Apache Tomcat, you need to download and import the management pack that supports the application, service, and OS.

Knowledge is defined in the management pack, which describes how to monitor the individual dependencies and components. Both Azure management packs require performing a set of configuration steps in Azure and Operations Manager before you can begin monitoring these resources.

At the application tier, Operations Manager offers basic application performance monitoring capabilities for some

legacy versions of .NET and Java. If certain applications within your hybrid cloud environment operate in an offline or network-isolated mode, such that they can't communicate with a public cloud service, Operations Manager Application Performance Monitoring (APM) might be a viable option for certain limited scenarios. For applications that are not running on legacy platforms but are hosted both on-premises and in any public cloud that allows communication through a firewall (either direct or via a proxy) to Azure, use Azure Monitor Application Insights. This service offers deep, code-level monitoring, with first-class support for ASP.NET, ASP.NET Core, Java, JavaScript, and Node.js.

For any web application that can be reached externally, you should enable a type of synthetic transaction known as [availability monitoring](#). It's important to know whether your application or a critical HTTP/HTTPS endpoint that your app relies on, is available and responsive. With Application Insights availability monitoring, you can run tests from multiple Azure datacenters and provide insight into the health of your application from a global perspective.

Although Operations Manager is capable of monitoring resources that are hosted in Azure, there are several advantages to including Azure Monitor, because its strengths overcome the limitations in Operations Manager and can establish a strong foundation to support eventual migration from it. Here we review each of those strengths and weaknesses, with our recommendation to include Azure Monitor in your hybrid monitoring strategy.

#### **Disadvantages of using Operations Manager by itself**

- Analyzing monitoring data in Operations Manager is commonly performed by using predefined views that are provided by management packs accessed from the console, from SQL Server Reporting Services (SSRS) reports, or from custom views that end users have created. Ad hoc data analysis isn't possible out of the box. Operations Manager reporting is inflexible. The data warehouse that provides long-term retention of the monitoring data doesn't scale or perform well. And expertise in writing T-SQL statements, developing a Power BI solution, or using third-party solutions is required to support the requirements for the various personas in the IT organization.
- Alerting in Operations Manager doesn't support complex expressions or include correlation logic. To help reduce noise, alerts are grouped to show the relationships between them and to identify their causes.

#### **Advantages of using Operations Manager with Azure Monitor**

- Azure Monitor is the way to work around the limitations of Operations Manager. It complements the Operations Manager data warehouse database by collecting important performance and log data. Azure Monitor delivers better analytics, performance (when querying large data volume), and retention than the Operations Manager data warehouse.

With the Azure Monitor Logs query language, you can create much more complex and sophisticated queries. You can run queries across terabytes of data in seconds. You can quickly transform your data into pie charts, time charts, and many other visualizations. To analyze this data, you're no longer constrained by working with Operations Manager reports that are based on SQL Server Reporting Services, custom SQL queries, or other workarounds.

- You can deliver an improved alerting experience by implementing the Azure Monitor Alerts Management solution. Alerts that are generated in the Operations Manager management group can be forwarded to the Azure Monitor Logs Analytics workspace. You can configure the subscription that's responsible for forwarding alerts from Operations Manager to Azure Monitor Logs to forward only certain alerts. For example, you can forward only alerts that meet your criteria for querying in support of problem management for trends, and investigation of the root cause of failures or problems, through a single pane of glass. Additionally, you can correlate other log data from Application Insights or other sources, to gain insight that help improve user experience, increase uptime, and reduce time to resolve incidents.
- You can monitor cloud-native infrastructure and applications, from a simple or multitier architecture in Azure using Azure Monitor, and you can use Operations Manager to monitor on-premises infrastructure. This monitoring includes one or more VMs, multiple VMs placed in an availability set or virtual machine scale set, or a containerized application deployed to Azure Kubernetes Service (AKS) that's running on Windows Server or Linux containers.

If you need comprehensive monitoring of Microsoft or third-party workloads running on your Azure VMs, and you have advanced scenarios that cannot be evaluated based on log or performance data alone, use System Center Operations Manager. Its management packs delivers advanced logic, which includes a service and health model, to determine the operational health of the workload.

- By using the Map feature of Azure Monitor for VMs, you can monitor standard connectivity metrics from network connections between your Azure VMs and on-premises VMs. These metrics include response time, requests per minute, traffic throughput, and links. You can identify failed connections, troubleshoot, perform migration validation, perform security analysis, and verify the overall architecture of the service. Map can automatically discover application components on Windows and Linux systems, and map the communication between services. This automation helps you identify connections and dependencies you were unaware of, plan and validate migration to Azure, and minimize speculation during incident resolution.
- By using Network Performance Monitor, you can monitor the network connectivity between:
  - Your corporate network and Azure.
  - Mission-critical multitier applications and microservices.
  - User locations and web-based applications (HTTP/HTTPS).

This strategy delivers visibility of the network layer, without the need for SNMP. It can also present, in an interactive topology map, the hop-by-hop topology of routes between the source and destination endpoint. It's a better choice than attempting to accomplish the same result with network monitoring in Operations Manager or with other network monitoring tools currently used in your environment.

## Monitor with Azure Monitor

Although a migration to the cloud presents numerous challenges, it also provides opportunities. It enables your organization to migrate from one or more on-premises enterprise monitoring tools to not only potentially reduce capital expenditures and operating costs, but also to benefit from the advantages that a cloud monitoring platform such as Azure Monitor can deliver at cloud scale. Examine your monitoring and alerting requirements, configuration of existing monitoring tools, and workloads transitioning to the cloud. After your plan is finalized, configure Azure Monitor.

- Monitor the hybrid infrastructure and applications, from a simple or multitier architecture where components are hosted between Azure, other cloud providers, and your corporate network. The components might include one or more VMs, multiple VMs placed in an availability set or virtual machine scale set, or a containerized application that's deployed to Azure Kubernetes Service (AKS) running on Windows Server or Linux containers.
- Use [Azure Arc](#) to prepare your servers, virtual machines, Kubernetes clusters, and databases across your environment for management as if they are running in Azure. Azure Arc delivers consistent inventory, management, governance, and security with familiar Azure services and management capabilities.
- Enable Azure Monitor for VMs, Azure Monitor for containers, and Application Insights to detect and diagnose issues between infrastructure and applications. For a more thorough analysis and correlation of data collected from the multiple components or dependencies supporting the application, you need to use Azure Monitor Logs.
- Create intelligent alerts that apply to a core set of applications and service components, help reduce alert noise with dynamic thresholds for complex signals, and use alert aggregation based on machine learning algorithms to help identify the issue quickly.
- Define a library of queries and dashboards to support the requirements of the various personas in the IT organization.
- Define standards and methods for enabling monitoring across the hybrid and cloud resources, a

monitoring baseline for each resource, alert thresholds, and so on.

- Configure role-based access control (RBAC) so you grant users and groups only the access required to monitor data from the resources they manage.
- Include automation and self-service to enable each team to create, enable, and tune their monitoring and alerting configurations as needed.

## Private cloud monitoring

You can achieve holistic monitoring of Azure Stack with System Center Operations Manager. Specifically, you can monitor the workloads that are running in the tenant, the resource level, on the virtual machines, and the infrastructure hosting Azure Stack (physical servers and network switches).

You can also achieve holistic monitoring with a combination of [infrastructure monitoring capabilities](#) that are included in Azure Stack. These capabilities help you view health and alerts for an Azure Stack region and the [Azure Monitor service](#) in Azure Stack, which provides base-level infrastructure metrics and logs for most services.

If you've already invested in Operations Manager, use the Azure Stack management pack to monitor the availability and health state of Azure Stack deployments, including regions, resource providers, updates, update runs, scale units, unit nodes, infrastructure roles, and their instances (logical entities comprised of the hardware resources). This management pack uses the Health and Update resource provider REST APIs to communicate with Azure Stack. To monitor physical servers and storage devices, use the OEM vendors' management pack (for example, provided by Lenovo, Hewlett Packard, or Dell). Operations Manager can natively monitor the network switches to collect basic statistics by using SNMP. Monitoring the tenant workloads is possible with the Azure management pack by following two basic steps. Configure the subscription that you want to monitor, and then add the monitors for that subscription.

## Next steps

[Collect the right data](#)

# Cloud monitoring guide: Collect the right data

11/9/2020 • 2 minutes to read • [Edit Online](#)

This article describes some considerations for collecting monitoring data in a cloud application.

To observe the health and availability of your cloud solution, you must configure the monitoring tools to collect a level of signals that are based on predictable failure states. These signals are the symptoms of the failure, not the cause. The monitoring tools use metrics and, for advanced diagnostics and root cause analysis, logs.

Plan for monitoring and migration carefully. Start by including the monitoring service owner, the manager of operations, and other related personnel during the Plan phase, and continue engaging them throughout the development and release cycle. Their focus will be to develop a monitoring configuration that's based on the following criteria:

- What is the composition of the service? Are those dependencies monitored today? If so, are there multiple tools involved? Is there an opportunity to consolidate, without introducing risks?
- What is the SLA of the service, and how will I measure and report it?
- What should the service dashboard look like when an incident is raised? What should the dashboard look like for the service owner, and for the team that supports the service?
- What metrics does the resource produce that I need to monitor?
- How will the service owner, support teams, and other personnel be searching the logs?

How you answer those questions, and the criteria for alerting, determines how you'll use the monitoring platform. If you're migrating from an existing monitoring platform or set of monitoring tools, use the migration as an opportunity to reevaluate the signals you collect. This is especially true now that there are several cost factors to consider when you migrate or integrate with a cloud-based monitoring platform like Azure Monitor. Remember, monitoring data needs to be actionable. You need to have optimized data collected to give you "a 10,000 foot view" of the overall health of the service. The instrumentation that's defined to identify real incidents should be as simple, predictable, and reliable as possible.

## Develop a monitoring configuration

The monitoring service owner and team typically follow a common set of activities to develop a monitoring configuration. These activities start at the initial planning stages, continue through testing and validating in a nonproduction environment, and extend to deploying into production. Monitoring configurations are derived from known failure modes, test results of simulated failures, and the experience of several people in the organization (the service desk, operations, engineers, and developers). Such configurations assume that the service already exists, it's being migrated to the cloud, and it hasn't been rearchitected.

For service-level quality results, monitor the health and availability of these services early in the development process. If you monitor the design of that service or application as an afterthought, your results won't be as successful.

To drive quicker resolution of the incident, consider the following recommendations:

- Define a dashboard for each service component.
- Use metrics to help guide further diagnosis and to identify a resolution or workaround of the issue if a root cause can't be uncovered.
- Use dashboard drill-down capabilities, or support customizing the view to refine it.
- If you need verbose logs, metrics should have helped target the search criteria. If the metrics didn't help, improve them for the next incident.

Embracing this guiding set of principles can help give you near-real-time insights, as well as better management of your service.

## Next steps

[Alerting strategy](#)

# Cloud monitoring guide: Alerting

11/9/2020 • 11 minutes to read • [Edit Online](#)

For years, IT organizations have struggled to combat the alert fatigue that's created by the monitoring tools deployed in the enterprise. Many systems generate a high volume of alerts often considered meaningless, while other alerts are relevant but are either overlooked or ignored. As a result, IT and developer operations have struggled to meet the service-level quality promised to internal or external customers. To ensure reliability, it's essential to understand the state of your infrastructure and applications. To minimize service degradation and disruption, or to decrease the effect of or reduce the number of incidents, you need to identify causes quickly.

## Successful alerting strategy

*You can't fix what you don't know is broken.*

Alerting on what matters is critical. It's underpinned by collecting and measuring the right metrics and logs. You also need a monitoring tool capable of storing, aggregating, visualizing, analyzing, and initiating an automated response when conditions are met. You can improve the observability of your services and applications only if you fully understand its composition. You map that composition into a detailed monitoring configuration to be applied by the monitoring platform. This configuration includes the predictable failure states (the symptoms, not the cause of the failure) that make sense to alert for.

Consider the following principles for determining whether a symptom is an appropriate candidate for alerting:

- **Does it matter?** Is the issue symptomatic of a real problem or issue influencing the overall health of the application? For example, do you care whether the CPU utilization is high on the resource? Or that a particular SQL query running on a SQL database instance on that resource is consuming high CPU utilization over a sustained period? Because the CPU utilization condition is a real issue, you should alert on it. But you don't need to notify the team, because it doesn't help point to what is causing the condition in the first place. Alerting and notifying on the SQL query process utilization issue is both relevant and actionable.
- **Is it urgent?** Is the issue real, and does it need urgent attention? If so, the responsible team should be immediately notified.
- **Are your customers affected?** Are users of the service or application affected as a result of the issue?
- **Are other dependent systems affected?** Are there alerts from dependencies that are interrelated, and that can possibly be correlated to avoid notifying different teams all working on the same problem?

Ask these questions when you're initially developing a monitoring configuration. Test and validate the assumptions in a nonproduction environment, and then deploy into production. Monitoring configurations are derived from known failure modes, test results of simulated failures, and experience from different members of the team.

After the release of your monitoring configuration, you can learn a lot about what's working and what's not. Consider high alert volume, issues unnoticed by monitoring but noticed by end users, and what were the best actions to have taken as part of this evaluation. Identify changes to implement to improve service delivery, as part of an ongoing, continuous monitoring improvement process. It's not just about evaluating alert noise or missed alerts, but also the effectiveness of how you're monitoring the workload. It's about the effectiveness of your alert policies, process, and overall culture to determine whether you're improving.

Both System Center Operations Manager and Azure Monitor support alerts based on static or even dynamic thresholds and actions set up on top of them. Examples include alerts for email, SMS, and voice calls for simple notifications. Both of these services also support IT Service Management (ITSM) integration, to automate the creation of incident records and escalate to the correct support team, or any other alert management system that uses a webhook.

When possible, you can use any of several services to automate recovery actions. These include System Center Orchestrator, Azure Automation, Azure Logic Apps, or autoscaling in the case of elastic workloads. While notifying the responsible teams is the most common action for alerting, automating corrective actions might also be appropriate. This automation can help streamline the entire incident management process. Automating these recovery tasks can also reduce the risk of human error.

## Azure Monitor alerting

If you're using Azure Monitor exclusively, follow these guidelines as you consider speed, cost, and storage volume.

Depending on the feature and configuration you're using, you can store monitoring data in any of six repositories:

- **Azure Monitor metrics database:** A time-series database used primarily for Azure Monitor platform metrics, but also has Application Insights metric data mirrored into it. Information entering this database has the fastest alert times.
- **Application Insights resource:** A database that stores most Application Insights telemetry in log form.
- **Azure Monitor Log Analytics workspace:** The primary store for Azure log data. Other tools can route data to it and can be analyzed in Azure Monitor Logs. Because of ingestion and indexing, log alert queries have higher latency. This latency is generally 5-10 minutes, but can be higher under certain circumstances.
- **Activity log:** Used for all activity log and service health events. Dedicated alerting is possible. Holds subscription level events that occur on objects in your subscription, as seen from the outside of those objects. An example might be when a policy is set or a resource is accessed or deleted.
- **Azure Storage:** General-purpose storage that's supported by Azure Diagnostics and other monitoring tools. It's a low-cost option for long-term retention of monitoring telemetry. Alerting isn't supported from data that's stored in this service.
- **Event Hubs:** Generally used to stream data into on-premises or other partners' monitoring or ITSM tools.

Azure Monitor has four types of alerts, each somewhat tied to the repository that the data is stored in:

- **Metric alert:** Alerts on metric data in Azure Monitor. Alerts occur when a monitored value crosses a user-defined threshold, and then again when it returns to "normal" state.
- **Log query alert:** Available to alert on log data from Application Insights or Azure Monitor Logs. It can also alert based on cross-workspace queries.
- **Activity log alert:** Alerts on items in the activity log, with the exception of Azure Service Health data.
- **Azure Service Health alert:** A special type of alert that's used only for Azure Service Health issues that come from the activity log, such as outages and upcoming planned maintenance. Note that this type of alert is configured through [Azure Service Health](#), a companion service to Azure Monitor.

### Enable alerting through partner tools

If you're using an external alerting solution, route as much as you can through Azure Event Hubs, which is the fastest path out of Azure Monitor. You'll have to pay for ingestion into Event Hub. If cost is an issue and speed isn't, you can use Azure Storage as a less expensive alternative. Just make sure that your monitoring or ITSM tools can read Azure Storage to extract the data.

Azure Monitor includes support for integrating with other monitoring platforms, and ITSM software such as ServiceNow. You can use Azure alerting and still trigger actions outside of Azure, as required by your incident management or DevOps process. If you want to alert in Azure Monitor and automate the response, you can initiate automated actions by using Azure Functions, Azure Logic Apps, or Azure Automation, based on your scenario and requirements.

## Specialized Azure monitoring offerings

Management solutions generally store their data Azure Monitor Logs. Two exceptions are Azure Monitor for VMs and Azure Monitor for containers. The following table describes the alerting experience based on the particular data type and where it is stored.

SOLUTION	DATA TYPE	ALERT BEHAVIOR
Azure Monitor for containers	Calculated average performance data from nodes and pods are written to the metrics database.	Create metric alerts if you want to be alerted based on variation of measured utilization performance, aggregated over time.
	Calculated performance data that uses percentiles from nodes, controllers, containers, and pods are written to the workspace. Container logs and inventory information are also written to the workspace.	Create log query alerts if you want to be alerted based on variation of measured utilization from clusters and containers. Log query alerts can also be configured based on pod-phase counts and status node counts.
Azure Monitor for VMs	Health criteria are metrics stored in the metrics database.	Alerts are generated when the health state changes from healthy to unhealthy. This alert supports only Action Groups that are configured to send SMS or email notifications.
	Map and guest operating system performance log data is written to the Log Analytics workspace.	Create log query alerts.

## Fastest speed driven by cost

Latency is one of the most critical decisions driving alerting and a quick resolution of issues affecting your service. If you require near-real-time alerting under five minutes, evaluate first if you have or can get alerts on your telemetry where it is stored by default. In general, this strategy is also the cheapest option, because the tool you're using is already sending its data to that location.

That said, there are some important footnotes to this rule.

Guest OS telemetry has multiple paths to get into the system.

- The fastest way to alert on this data is to import it as custom metrics. Do this by using the Azure Diagnostics extension and then using a metric alert. However, custom metrics are currently in preview and are [more expensive than other options](#).
- The least expensive, but with some ingestion latency, is to send it to a Log Analytics workspace. Running the Log Analytics agent on the VM is the best way to get all guest operating system metric and log data into the workspace.
- You can send it for storage as a metric and a log in Azure Monitor by running both the Diagnostic extension and the Log Analytics agent on the same VM. You can then alert quicker, but also use the guest operating system data as part of more complex queries when you combine it with other telemetry.

**Importing data from on-premises:** If you're trying to query and monitor across machines running in Azure and on-premises, you can use the Log Analytics agent to collect guest operating system data. You can then use a feature called [logs to metrics](#) to collect and store as metrics in Azure Monitor. This method bypasses part of the ingestion process into Azure Monitor Logs, and the data is thus available sooner.

## Minimize alerts

If you use a solution such as Azure Monitor for VMs and find the default health criteria that monitors performance utilization acceptable, don't create overlapping metric or log query alerts based on the same performance counters.

If you aren't using Azure Monitor for VMs, make the job of creating alerts and managing notifications easier by exploring the following features:

#### **NOTE**

These features apply only to metric alerts, alerts based on data that's being sent to the Azure Monitor metric database. The features don't apply to the other types of alerts. As mentioned previously, the primary objective of metric alerts is speed. If getting an alert in less than five minutes isn't of primary concern, you can use a log query alert instead.

- **Dynamic thresholds:** Dynamic thresholds look at the activity of the resource over a time period, and create upper and lower "normal behavior" thresholds. When the metric being monitored falls outside of these thresholds, you get an alert.
- **Multisignal alerts:** You can create a metric alert that uses the combination of two different inputs from two different resource types. For example, if you want to fire an alert when the CPU utilization of a VM is over 90 percent, and the number of messages in a certain Azure Service Bus queue feeding that VM exceeds a certain amount, you can do so without creating a log query. This feature works for only two signals. If you have a more complex query, feed your metric data into the Log Analytics workspace, and use a log query.
- **Multiresource alerts:** Azure Monitor allows a single metric alert rule that applies to all VM resources. This feature can save you time because you don't need to create individual alerts for each VM. Pricing for this type of alert is the same. Whether you create 50 alerts for monitoring CPU utilization for 50 VMs, or one alert that monitors CPU utilization for all 50 VMs, it costs you the same amount. You can use these types of alerts in combination with dynamic thresholds as well.

Used together, these features can save time by minimizing alert notifications and the management of the underlying alerts.

#### **Limits on alerts**

Be sure to note the [limits on the number of alerts you can create](#). Some limits (but not all of them) can be increased by calling support.

#### **Best query experience**

If you're looking for trends across all your data, it makes sense to import all your data into Azure Logs, unless it's already in Application Insights. You can create queries across both workspaces, so there's no need to move data between them. You can also import activity log and Azure Service Health data into your Log Analytics workspace. You pay for this ingestion and storage, but you get all your data in one place for analysis and querying. This approach also gives you the ability to create complex query conditions and alert on them.

# Cloud monitoring guide: Monitoring platforms overview

11/9/2020 • 14 minutes to read • [Edit Online](#)

Microsoft provides a range of monitoring capabilities from two products: System Center Operations Manager, which was designed for on-premises and then extended to the cloud, and Azure Monitor, which was designed for the cloud but can also monitor on-premises systems. These two offerings deliver core monitoring services, such as alerting, service uptime tracking, application and infrastructure health monitoring, diagnostics, and analytics.

Many organizations are embracing the latest practices for DevOps agility and cloud innovations to manage their heterogeneous environments. Yet they are also concerned about their ability to make appropriate and responsible decisions about how to monitor those workloads.

This article provides a high-level overview of our monitoring platforms to help you understand how each delivers core monitoring functionality.

## The story of System Center Operations Manager

In 2000, we entered the operations management field with Microsoft Operations Manager 2000. In 2007, we introduced a reengineered version of the product, System Center Operations Manager. It moved beyond simple monitoring of a Windows server and concentrated on robust, end-to-end service and application monitoring, including heterogeneous platforms, network devices, and other application or service dependencies. It's an established, enterprise-grade monitoring platform for on-premises environments, in the same class as IBM Tivoli or HP Operations Manager in the industry. It has grown to support monitoring compute and platform resources running in Azure, Amazon Web Services (AWS), and other cloud providers.

## The story of Azure Monitor

When Azure was released in 2010, monitoring of cloud services was provided with the Azure Diagnostics agent, which provided a way to collect diagnostics data from Azure resources. This capability was considered a general monitoring tool rather than an enterprise-class monitoring platform.

Application Insights was introduced to shift with changes in the industry where proliferation of cloud, mobile, and IoT devices was growing and the introduction of DevOps practices. It grew from Application Performance Monitoring in Operations Manager to a service in Azure, where it delivers rich monitoring of web applications written in a variety of languages. In 2015, the preview of Application Insights for Visual Studio was announced and later, it became known as just Application Insights. It collects details about application performance, requests and exceptions, and traces.

In 2015, Azure Operational Insights was made generally available. It delivered the Log Analytics analysis service that collected and searched data from machines in Azure, on-premises, or other cloud environments, and connected to System Center Operations Manager. Intelligence packs were offered that delivered a variety of prepackaged management and monitoring configurations that contained a collection of query and analytic logic, visualizations, and data collection rules for such scenarios as security auditing, health assessments, and alert management. Later, Azure Operational Insights became known as Log Analytics.

In 2016, the preview of Azure Monitor was announced at the Microsoft Ignite conference. It provided a common framework to collect platform metrics, resource diagnostics logs, and subscription-level activity log events from any Azure service that started using the framework. Previously, each Azure service had its own monitoring method.

At the 2018 Ignite conference, we announced that the Azure Monitor brand expanded to include several different services originally developed with independent functionality:

- The original **Azure Monitor**, for collecting platform metrics, resource diagnostics logs, and activity logs for Azure platform resources only.
- **Application Insights**, for application monitoring.
- **Log Analytics**, the primary location for collecting and analyzing log data.
- A new **unified alerting service**, which brought together alert mechanisms from each of the other services mentioned earlier.
- **Azure Network Watcher**, for monitoring, diagnosing, and viewing metrics for resources in a virtual network.

## The story of Operations Management Suite (OMS)

From 2015 until April 2018, Operations Management Suite (OMS) was a bundling of the following Azure management services for licensing purposes:

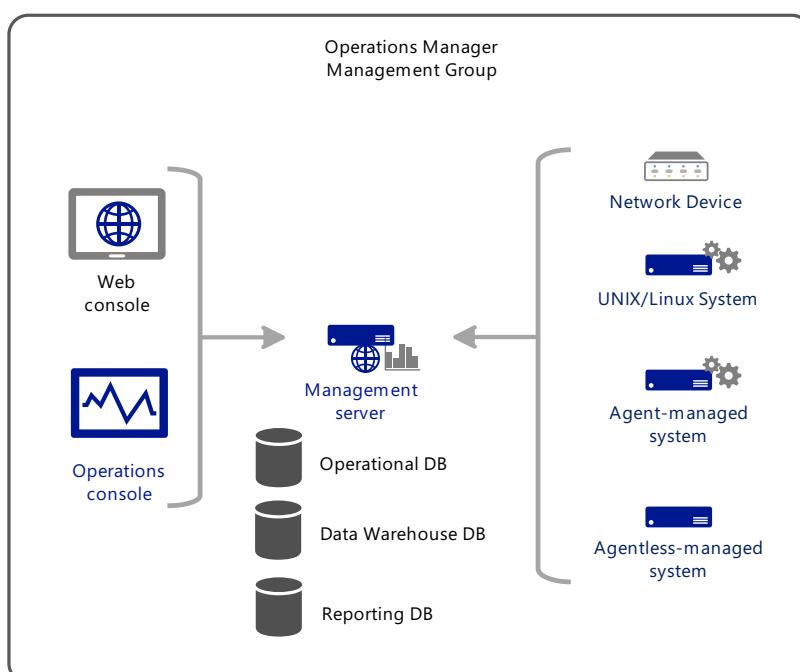
- Application Insights
- Azure Automation
- Azure Backup
- Operational Insights (later rebranded as Log Analytics)
- Site Recovery

The functionality of the services that were part of OMS did not change when OMS was discontinued. They were realigned under Azure Monitor.

## Infrastructure requirements

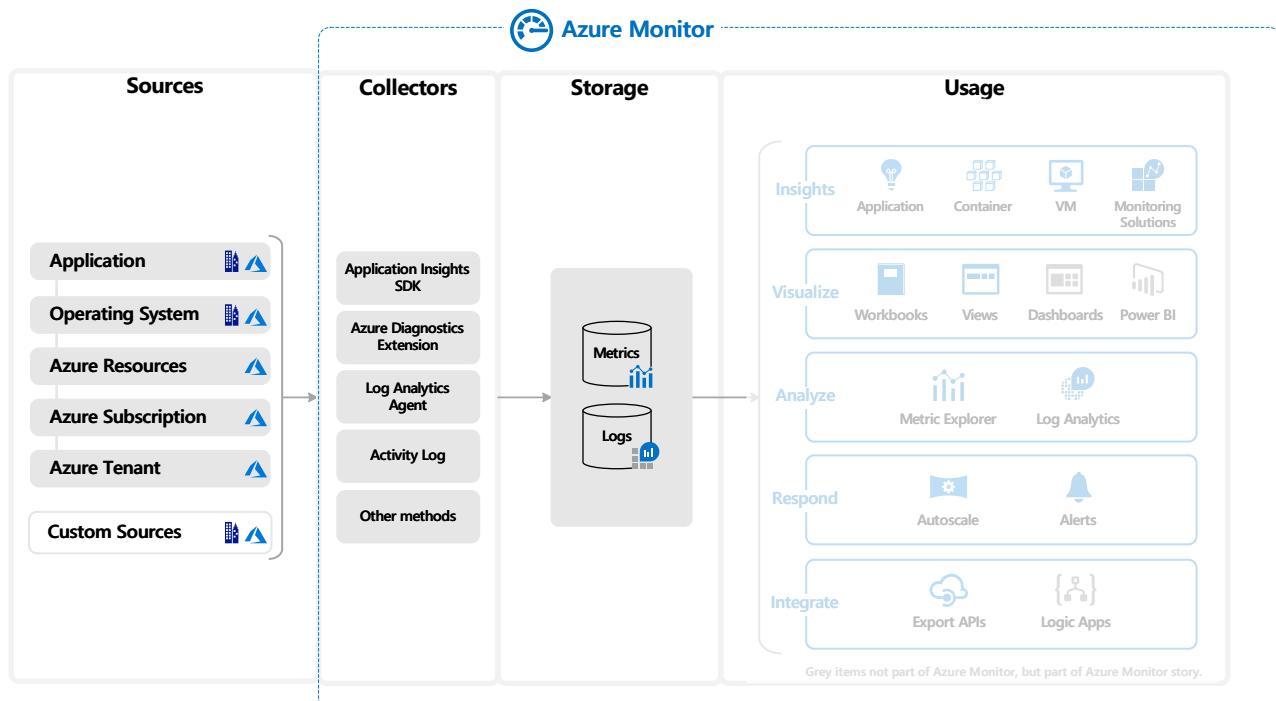
### Operations Manager

Operations Manager requires significant infrastructure and maintenance to support a management group, which is a basic unit of functionality. At a minimum, a management group consists of one or more management servers, a SQL Server instance, hosting the operational and reporting data warehouse database, and agents. The complexity of a management group design depends on multiple factors, such as the scope of workloads to monitor, and the number of devices or computers supporting the workloads. If you require high availability and site resiliency, as is commonly the case with enterprise monitoring platforms, the infrastructure requirements and associated maintenance can increase dramatically.



## Azure Monitor

Azure Monitor is a software as a service (SaaS) offering, so its supporting infrastructure runs in Azure and is managed by Microsoft. It performs monitoring, analytics, and diagnostics at scale. It is available in all national clouds. Core parts of the infrastructure (collectors, metrics and logs store, and analytics) that support Azure Monitor are maintained by Microsoft.

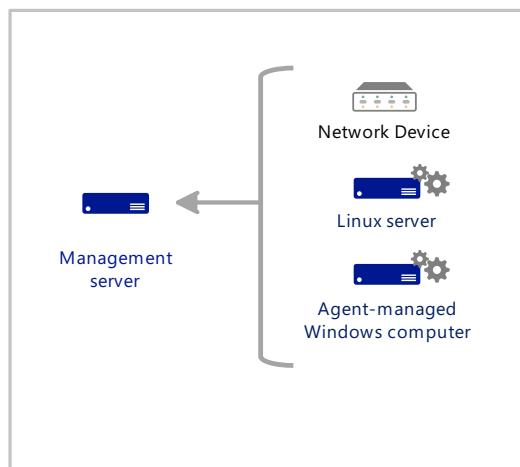


## Data collection

### Operations Manager

#### Agents

Operations Manager collects data directly only from agents that are installed on [Windows computers](#). It can accept data from the Operations Manager SDK, but this approach is typically used for partners that extend the product with custom applications, not for collecting monitoring data. It can collect data from other sources, such as [Linux computers](#) and network devices, by using special modules that run on the Windows agent that remotely accesses these other devices.



The Operations Manager agent can collect from multiple data sources on the local computer, such as the event log, custom logs, and performance counters. It can also run scripts, which can collect data from the local computer or from external sources. You can write custom scripts to collect data that can't be collected by other means, or to collect data from a variety of remote devices that can't otherwise be monitored.

#### Management packs

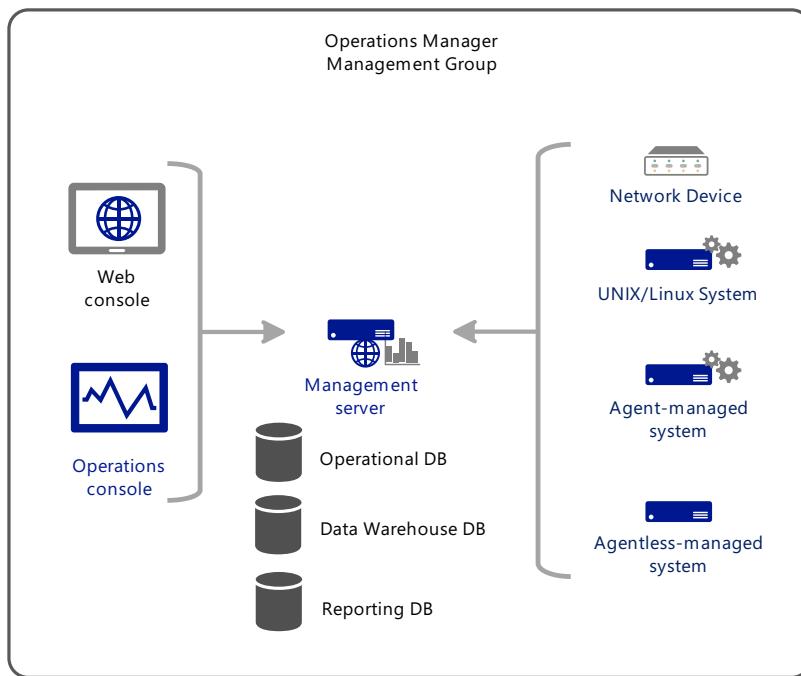
Operations Manager performs all monitoring with workflows (rules, monitors, and object discoveries). These workflows are packaged together in a [management pack](#) and deployed to agents. Management packs are available for a variety of products and services, which include predefined rules and monitors. You can also author your own management pack for your own applications and custom scenarios.

#### Monitoring configuration

Management packs can contain hundreds of rules, monitors, and object discovery rules. An agent runs all these monitoring settings from all the management packs that apply, which are determined by discovery rules. Each instance of each monitoring setting runs independently and acts immediately on the data that it collects. This is how Operations Manager can achieve near-real-time alerting and the current health state of monitored resources.

For example, a monitor might sample a performance counter every few minutes. If that counter exceeds a threshold, it immediately sets the health state of its target object, which immediately triggers an alert in the management group. A scheduled rule might watch for a particular event to be created and immediately fire an alert when that event is created in the local event log.

Because these monitoring settings are isolated from each other and work from the individual sources of data, Operations Manager has challenges correlating data between multiple sources. It's also difficult to react to data after it's been collected. You can run workflows that access the Operations Manager database, but this scenario isn't common, and it's typically used for a limited number of special purpose workflows.



## Azure Monitor

#### Data sources

Azure Monitor collects data from a variety of sources, including Azure infrastructure and platform resources, agents on Windows and Linux computers, and monitoring data collected in Azure storage. Any REST client can write log data to Azure Monitor by using an API, and you can define custom metrics for your web applications. Some metric data can be routed to different locations, depending on its usage. For example, you might use the data for "fast-as-possible" alerting or for long-term trend analysis searches in conjunction with other log data.

#### Monitoring solutions and insights

Monitoring solutions use the logs platform in Azure Monitor to provide monitoring for a particular application or service. They typically define data collection from agents or from Azure services, and provide log queries and views to analyze that data. They typically don't provide alert rules, which means that you must define your own alert criteria based on collected data.

Insights, such as Azure Monitor for containers and Azure Monitor for VMs, use the logs and metrics platform of Azure Monitor to provide a customized monitoring experience for an application or service in the Azure portal.

They might provide health monitoring and alerting conditions, in addition to customized analysis of collected data.

#### **Monitoring configuration**

Azure Monitor separates data collection from actions taken against that data, which supports distributed microservices in a cloud environment. It consolidates data from multiple sources into a common data platform, and provides analysis, visualization, and alerting capabilities based on the collected data.

Data collected by Azure Monitor is stored as either logs or metrics, and different features of Azure Monitor rely on either. Metrics contain numerical values in time series that are well suited for near-real-time alerting and quick detection of issues. Logs contain text or numerical data and can be queried using a powerful language especially useful for performing complex analysis.

Because Azure Monitor separates data collection from actions against that data, it might be unable to provide near-real-time alerting in many cases. To alert on log data, queries are run on a recurring schedule defined in the alert. This behavior allows Azure Monitor to easily correlate data from all monitored sources, and you can interactively analyze data in a variety of ways. This is especially helpful for doing root cause analysis and identifying where else an issue might occur.

## Health monitoring

#### **Operations Manager**

Management Packs in Operations Manager include a service model that describes the components of the application being monitored and their relationship. Monitors identify the current health state of each component based on data and scripts on the agent. Health states roll up so that you can quickly view the summarized health state of monitored computers and applications.

#### **Azure Monitor**

Azure Monitor doesn't provide a user-definable method of implementing a service model or monitors that indicate the current health state of any service components. Because monitoring solutions are based on standard features of Azure Monitor, they don't provide state-level monitoring. The following features of Azure Monitor can be helpful:

- **Application Insights:** Builds a composite map of your web application, and provides a health state for each application component or dependency. This includes alerts status and drill-down to more detailed diagnostics of your application.
- **Azure Monitor for VMs:** Delivers a health-monitoring experience for the guest Azure VMs, similar to that of Operations Manager, when it monitors Windows and Linux virtual machines. It evaluates the health of key operating system components from the perspective of availability and performance to determine the current health state. When it determines that the guest VM is experiencing sustained resource utilization, disk-space capacity, or an issue related to core operating system functionality, it generates an alert to bring this state to your attention.
- **Azure Monitor for containers:** Monitors the performance and health of Azure Kubernetes Service or Azure Container Instances. It collects memory and processor metrics from controllers, nodes, and containers that are available in Kubernetes through the Metrics API. It also collects container logs and inventory data about containers and their images. Predefined health criteria that are based on the collected performance data help you identify whether a resource bottleneck or capacity issue exists. You can also understand the overall performance, or the performance from a specific Kubernetes object type (pod, node, controller, or container).

## Analyze data

#### **Operations Manager**

Operations Manager provides four basic ways to analyze data after it has been collected:

- **Health Explorer:** Helps you discover which monitors are identifying a health state issue and review knowledge about the monitor and possible causes for actions related to it.
- **Views:** Offers predefined visualizations of collected data, such as a graph of performance data or a list of monitored components and their current health state. Diagram views visually present the service model of an application.
- **Reports:** Allow you to summarize historical data that's stored in the Operations Manager data warehouse. You can customize the data that views and reports are based on. However, there is no feature to allow for complex or interactive analysis of collected data.
- **Operations Manager Command Shell:** Extends Windows PowerShell with an additional set of cmdlets, and can query and visualize collected data. This includes graphs and other visualizations, natively with PowerShell, or with the Operations Manager HTML-based web console.

## Azure Monitor

With the powerful Azure Monitor analytics engine, you can interactively work with log data and combine them with other monitoring data for trending and other data analysis. Views and dashboards allow you to visualize query data in a variety of ways from the Azure portal, and import it into Power BI. Monitoring solutions include queries and views to present the data they collect. Insights such as Application Insights, Azure Monitor for VMs, and Azure Monitor for containers include customized visualizations to support interactive monitoring scenarios.

# Alerting

## Operations Manager

Operations Manager creates alerts in response to predefined events, when a performance threshold is met, and when the health state of a monitored component changes. It includes the complete management of alerts, allowing you to set their resolution and assign them to various operators or system engineers. You can set notification rules that specify which alerts will send proactive notifications.

Management packs include various predefined alerting rules for different critical conditions in the application being monitored. You can tune these rules or create custom rules to the particular requirements of your environment.

## Azure Monitor

With Azure Monitor, you can create alerts based on a metric crossing a threshold, or based on a scheduled query result. Although alerts based on metrics can achieve near-real-time results, scheduled queries have a longer response time, depending on the speed of data ingestion and indexing. Instead of being limited to a specific agent, log query alerts in Azure Monitor let you analyze data across all data stored in multiple workspaces. These alerts also include data from a specific Application Insights application by using a cross-workspace query.

Although monitoring solutions can include alert rules, you ordinarily create them based on your own requirements.

# Workflows

## Operations Manager

Management packs in Operations Manager contain hundreds of individual workflows, and they determine both what data to collect and what action to perform with that data. For example, a rule might sample a performance counter every few minutes, storing its results for analysis. A monitor might sample the same performance counter and compare its value to a threshold to determine the health state of a monitored object. Another rule might run a script to collect and analyze some data on an agent computer, and then fire an alert if it returns a particular value.

Workflows in Operations Manager are independent of each other, which makes analysis across multiple monitored objects difficult. These monitoring scenarios must be based on data after it's collected, which is possible but can be

difficult, and it isn't common.

## Azure Monitor

Azure Monitor separates data collection from actions and analysis taken from that data. Agents and other data sources write log data to a Log Analytics workspace and write metric data to the metric database, without any analysis of that data or knowledge of how it might be used. Monitor performs alerting and other actions from the stored data, which allows you to perform analysis across data from all sources.

## Extend the base platform

### Operations Manager

Operations Manager implements all monitoring logic in a management pack, which you either create yourself or obtain from us or a partner. When you install a management pack, it automatically discovers components of the application or service on different agents, and deploys appropriate rules and monitors. The management pack contains health definitions, alert rules, performance and event collection rules, and views, to provide complete monitoring that supports the infrastructure service or application.

The Operations Manager SDK enables Operations Manager to integrate with third-party monitoring platforms or IT service management (ITSM) software. The SDK is also used by some partner management packs to support monitoring network devices and deliver custom presentation experiences, such as the Squared Up HTML5 dashboard or integration with Microsoft Office Visio.

### Azure Monitor

Azure Monitor collects metrics and logs from Azure resources, with little to no configuration. Monitoring solutions add logic for monitoring an application or service, but they still work within the standard log queries and views in Monitor. Insights, such as Application Insights and Azure Monitor for VMs, use the Monitor platform for data collecting and processing. They also provide additional tools to visualize and analyze the data. You can combine data collected by insights with other data, by using core Monitor features such as log queries and alerts.

Monitor supports several methods to collect monitoring or management data from Azure or external resources. You can then extract and forward data from the metric or log stores to your ITSM or monitoring tools. Or you can perform administrative tasks by using the Azure Monitor REST API.

## Next steps

[Monitoring the cloud deployment models](#)

# Skills readiness for cloud monitoring

11/9/2020 • 6 minutes to read • [Edit Online](#)

During the Plan phase of your migration journey, the objective is to develop the plans necessary to guide implementation. The plans need to also include how you will operate these workloads before they are transitioned or released into production, and not afterwards. Business stakeholders expect valuable services, and they expect them without disruption. IT staff members realize they need to learn new skills and adapt so they are prepared to confidently use the integrated Azure services to effectively monitor resources in Azure and hybrid environments.

Developing the necessary skills can be accelerated with the following learning paths. They are organized starting with learning the fundamentals and then divided across three primary subject domains - infrastructure, application, and data analysis.

## Fundamentals

- Introduction to [Azure Resource Manager](#) discusses the basic concepts of management and deployment of Azure resources. The IT staff managing the monitoring experience across the enterprise should understand management scopes, role-based access control (RBAC), using Azure Resource Manager templates, and management of resources using Azure CLI and Azure PowerShell.
- Introduction to [Azure Policy](#) helps you learn how you can use Azure Policy to create, assign, and manage policies. Azure Policy can deploy and configure the Azure Monitor agents, enable monitoring with Azure Monitor for VMs and Azure Security Center, deploy Diagnostic Settings, audit guest configuration settings, and more.
- Introduction to [Azure command-line interface \(CLI\)](#), which is our cross-platform command-line experience for managing Azure resources. Also review, introduction to [Azure PowerShell](#). As part of their beginner-level course, [Learning Azure Management Tools](#), LinkedIn offers sessions covering Azure CLI and PowerShell programming languages:
  - [Use the Azure CLI](#).
  - [Get started with Azure PowerShell](#)
- Learn how to secure resources using policy, role-based access control, and other Azure services by viewing [Implement resource management security in Azure](#).
- [Monitoring Microsoft Azure Resources and Workloads](#) helps you learn how to use Azure monitoring tools to monitor Azure network resources as well as resources located on-premises.
- Learn about planning and designing your monitoring deployments at-scale and automating actions by viewing [Azure Monitor best practices and recommendations](#).

## Infrastructure monitoring

- [Design a Monitoring Strategy for Infrastructure in Microsoft Azure](#) helps you learn foundational knowledge of monitoring capabilities and solutions in Azure.
- [How to monitor your Kubernetes clusters](#) provides an intermediate level deep dive to help you learn about monitoring your Kubernetes cluster with Azure Monitor for containers.
- Learn with Azure Monitor how to monitor data from [Azure Storage and HDInsight](#).
- [Microsoft Azure Database Monitoring Playbook](#) explores the key monitoring capabilities that can be used to

gain insight and actionable steps for Azure SQL Database, Azure SQL Data Warehouse, and Azure Cosmos DB.

- [Monitoring Microsoft Azure Hybrid Cloud Networks](#) is an advanced-level course that helps you learn how to use Azure monitoring tools to visualize, maintain, and optimize Azure virtual networks and virtual private network connections for your hybrid cloud implementation.
- With [Azure Arc for servers](#), learn how you can manage your Windows and Linux machines hosted outside of Azure similarly to how you manage native Azure virtual machines.
- [How to monitor your VMs](#) provides an intermediate level deep dive to help you learn about monitoring your hybrid machines or servers, and Azure VM or virtual machine scale sets with Azure Monitor for VMs.

## Application monitoring

- Understand how [Azure Monitor](#) helps you view availability and performance of your applications and services together from one place. Pluralsight offers the following courses to help:
  - [Microsoft Azure DevOps Engineer: Optimize Feedback Mechanisms](#) helps you prepare you to use Azure Monitor, including Application Insights, to monitor and optimize your web applications.
  - [Capture and view page load times in your Azure web app](#). Get started with this course on using Azure Monitor Application Insights for end-to-end monitoring of your applications components running in Azure.
  - [Microsoft Azure Database Monitoring Playbook](#) helps you learn how to implement and use monitoring of Azure SQL Database, Azure SQL Data Warehouse, and Azure Cosmos DB.
  - [Instrument Applications with Azure Monitor Application Insights](#) is a deep-dive course on using the Application Insights SDK to collect telemetry and events from an app with Angular and Node.js components.
  - [Application Debugging and Profiling](#) is a recording from a Microsoft conference session on using and interpreting data provided by the Azure Monitor Application Insights Snapshot Debugger and Profiler.

## Data analysis

- Learn how to write [log queries in Azure Monitor](#). The Kusto query language is the primary resource for writing Azure Monitor log queries to explore and analyze log data between the collected data from Azure and hybrid resource application dependencies, including the live application.
- [Kusto Query Language \(KQL\) from Scratch](#) is a comprehensive course that includes detailed examples covering a wide range of use-cases and techniques for log analysis in Azure Monitor logs.

## Deeper skills exploration

Beyond these initial options for developing skills, there are a variety of learning options available.

### Typical mappings of cloud IT roles

Microsoft and partners offer a variety of options for all audiences to develop their skills with Azure services:

- [Microsoft IT Pro Career Center](#): Serves as a free online resource to help map your cloud career path. Learn what industry experts suggest for your cloud role and the skills to get you there. Follow a learning curriculum at your own pace to build the skills you need most to stay relevant.

Turn your knowledge of Azure into official recognition with [Azure certification training and exams](#).

# Azure DevOps and Project Management

The hybrid cloud environment disrupts IT with undefined roles, responsibilities, and activities. Organizations must move to modern service management practices, including Agile and DevOps methodologies, to better meet the transformation and optimization needs of today's businesses in a streamlined and efficient manner.

As part of migrating to a cloud monitoring platform, the IT team responsible for managing monitoring in the enterprise need to include agile training and participation in DevOps activities. This also includes following the *Dev in DevOps* by taking requirements and turning into organized agile requirements, in order to deliver minimally viable monitoring solutions that are refined iteratively and in line with business needs. For source control to manage the iterative monitoring solution packages and any other related collateral, connect your Azure DevOps Server project with a GitHub Enterprise Server repository. This provides a link between GitHub commits and pull requests to work items. You can use GitHub Enterprise for development in support of continuous monitoring integration and deployment, while using Azure Boards to plan and track your work.

To learn more, review the following:

- [Get started with Azure DevOps](#).
- [Learn about DevOps dojo white belt foundation](#)
- [Evolve your DevOps practices](#)
- [Automate your deployments with Azure DevOps](#)

## Other Considerations

Customers often struggle to manage, maintain, and deliver the expected business (and to the IT organization) outcomes for the services that IT is charged with delivering. Monitoring is considered core to managing infrastructure and the business, with a focus on measuring quality of service and customer experience. In order to achieve those goals, lay the groundwork using ITSM in conjunction with DevOps, which will help the monitoring team mature how they manage, deliver, and support the monitoring service. Adopting an ITSM framework allows the monitoring team to function as a provider and gain recognition as a trusted business enabler by aligning to the strategic goals and needs of the organization.

Review the following to understand the updates made to the most popular ITSM framework [ITIL v4 and Cloud Computing whitepaper](#), which focuses on joining existing ITIL guidance with best practices from DevOps, Agile, and Lean. Also consider the [IT4IT reference architecture](#) that delivers an alternative blueprint on how to transform IT using a process agnostic framework.

## Learn more

To discover additional learning paths, browse the [Microsoft Learn catalog](#). Use the Roles filter to align learning paths with your role.

# Centralize management operations

11/9/2020 • 2 minutes to read • [Edit Online](#)

For most organizations, using a single Azure Active Directory (Azure AD) tenant for all users simplifies management operations and reduces maintenance costs. This is because all management tasks can be performed by designated users, user groups, or service principals within that tenant.

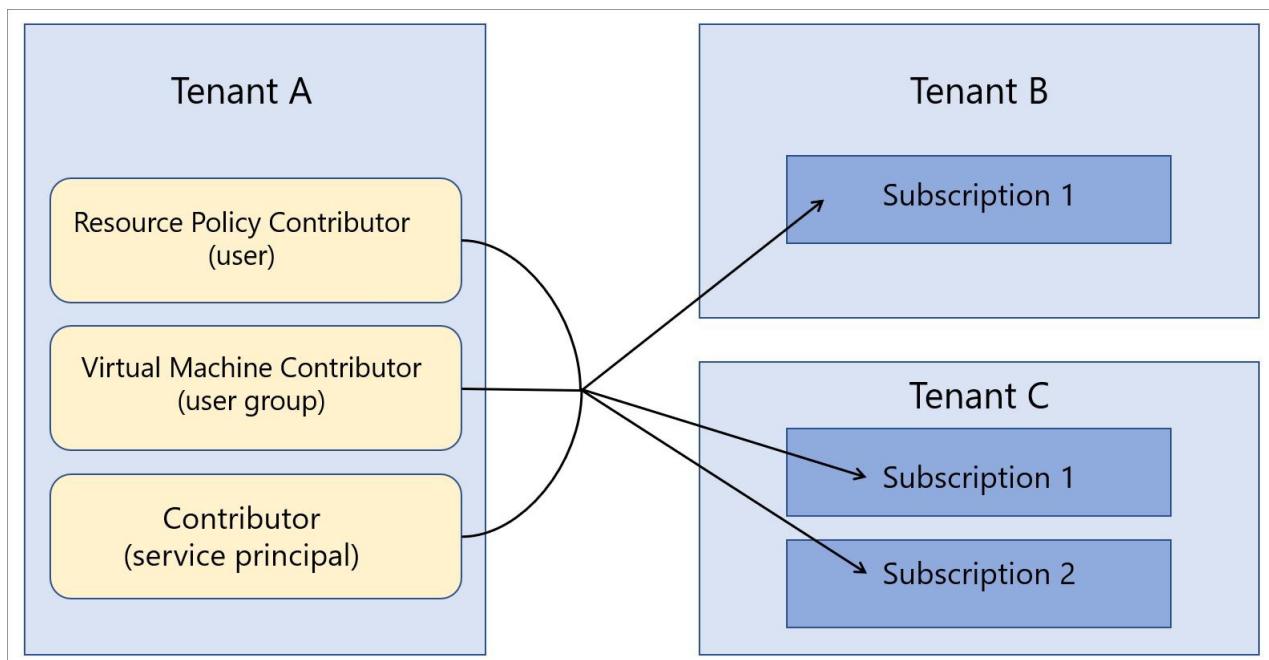
We recommend that you use only one Azure AD tenant for your organization, if possible. However, some situations might require an organization to maintain multiple Azure AD tenants for the following reasons:

- They are wholly independent subsidiaries.
- They're operating independently in multiple geographies.
- Certain legal or compliance requirements apply.
- There are acquisitions of other organizations (sometimes temporary until a long-term tenant consolidation strategy is defined).

When a multiple-tenant architecture is required, [Azure Lighthouse](#) provides a way to centralize and streamline management operations. Subscriptions from multiple tenants can be onboarded for [Azure delegated resource management](#). This option allows specified users in the managing tenant to perform [cross-tenant management functions](#) in a centralized and scalable manner.

For example, let's say your organization has a single tenant, **Tenant A**. The organization then acquires two additional tenants, **Tenant B** and **Tenant C**, and you have business reasons that require you to maintain them as separate tenants.

Your organization wants to use the same policy definitions, backup practices, and security processes across all tenants. Because you already have users (including user groups and service principals) that are responsible for performing these tasks within Tenant A, you can onboard all of the subscriptions within Tenant B and Tenant C so that those same users in Tenant A can perform those tasks. Tenant A then becomes the managing tenant for Tenant B and Tenant C.



For more information, see [Azure Lighthouse in enterprise scenarios](#).

# Establish an operational fitness review

11/9/2020 • 9 minutes to read • [Edit Online](#)

As your enterprise begins to operate workloads in Azure, the next step is to establish a process for *operational fitness review*. This process enumerates, implements, and iteratively reviews the *nonfunctional requirements* for these workloads. Nonfunctional requirements are related to the expected operational behavior of the service.

There are five essential categories of nonfunctional requirements, known as the [pillars of architecture excellence](#):

- Cost optimization
- Operational excellence
- Performance efficiency
- Reliability
- Security

A process for operational fitness review ensures that your mission-critical workloads meet the expectations of your business with respect to the pillars.

Create a process for operational fitness review to fully understand the problems that result from running workloads in a production environment, and how to remediate and resolve those problems. This article outlines a high-level process for operational fitness review that your enterprise can use to achieve this goal.

## Operational fitness at Microsoft

From the outset, many teams across Microsoft have been involved in the development of the Azure platform. It's difficult to ensure quality and consistency for a project of such size and complexity. You need a robust process to enumerate and implement fundamental nonfunctional requirements on a regular basis.

The processes that Microsoft follows form the basis for the processes outlined in this article.

## Understand the problem

As discussed in [Get started: Accelerate migration](#), the first step in an enterprise's digital transformation is to identify the business problems to be solved by adopting Azure. The next step is to determine a high-level solution to the problem, such as migrating a workload to the cloud or adapting an existing, on-premises service to include cloud functionality. Finally, you design and implement the solution.

During this process, the focus is often on the features of the service: the set of *functional* requirements that you want the service to perform. For example, a product-delivery service requires features for determining the source and destination locations of the product, tracking the product during delivery, and sending notifications to the customer.

The *nonfunctional* requirements, in contrast, relate to properties such as the service's [availability](#), [resiliency](#), and [scalability](#). These properties differ from the functional requirements because they don't directly affect the final function of any particular feature in the service. However, nonfunctional requirements do relate to the performance and continuity of the service.

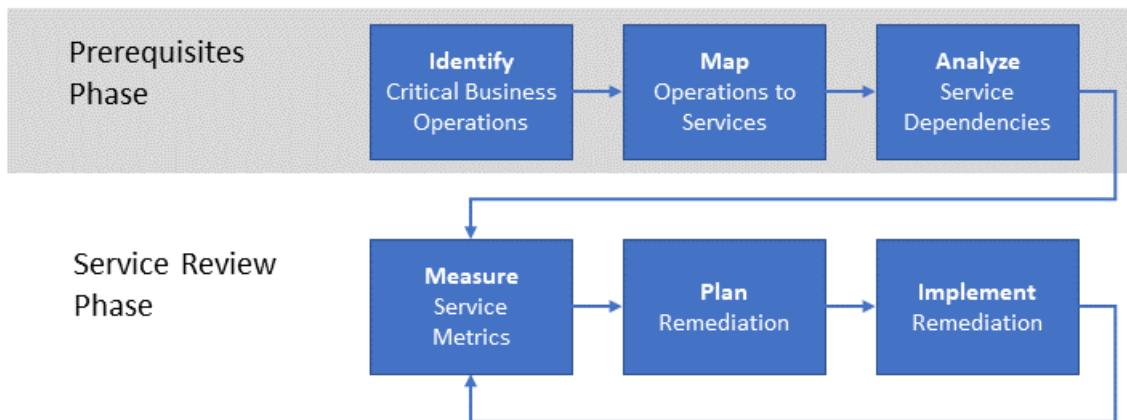
You can specify some nonfunctional requirements in terms of a service-level agreement (SLA). For example, you can express service continuity as a percentage of availability: "Available 99.99 percent of the time". Other nonfunctional requirements might be more difficult to define and might change as production needs change. For example, a consumer-oriented service might face unanticipated throughput requirements after a surge of popularity.

## NOTE

For more information about resiliency requirements, see [Designing reliable Azure applications](#). That article includes explanations of concepts like recovery-point objective (RPO), recovery-time objective (RTO), and SLA.

# Process for operational fitness review

The key to maintaining the performance and continuity of an enterprise's services is to implement a process for operational fitness review.



At a high level, the process has two phases. In the *prerequisites phase*, the requirements are established and mapped to supporting services. This phase occurs infrequently: perhaps annually or when new operations are introduced. The output of the prerequisites phase is used in the *flow phase*. The flow phase occurs more frequently, such as monthly.

## Prerequisites phase

The steps in this phase capture the requirements for conducting a regular review of the important services.

1. **Identify critical business operations.** Identify the enterprise's mission-critical business operations. Business operations are independent from any supporting service functionality. In other words, business operations represent the actual activities that the business needs to perform and that are supported by a set of IT services.  
The term *mission-critical* (or *business critical*) reflects a severe impact on the business if the operation is impeded. For example, an online retailer might have a business operation, such as "enable a customer to add an item to a shopping cart" or "process a credit card payment." If either of these operations fails, a customer can't complete the transaction and the enterprise fails to realize sales.
2. **Map operations to services.** Map the critical business operations to the services that support them. In the shopping-cart example, several services might be involved, including an inventory stock-management service and a shopping-cart service. To process a credit-card payment, an on-premises payment service might interact with a third-party, payment-processing service.
3. **Analyze service dependencies.** Most business operations require orchestration among multiple supporting services. It's important to understand the dependencies between the services, and the flow of mission-critical transactions through these services.

Also consider the dependencies between on-premises services and Azure services. In the shopping-cart example, the inventory stock-management service might be hosted on-premises and ingest data entered by employees from a physical warehouse. However, it might store data off-premises in an Azure service, such as [Azure Storage](#), or a database, such as [Azure Cosmos DB](#).

An output from these activities is a set of *scorecard metrics* for service operations. The scorecard measures criteria such as availability, scalability, and disaster recovery. Scorecard metrics express the operational criteria that you expect the service to meet. These metrics can be expressed at any level of granularity that's appropriate for the service operation.

The scorecard should be expressed in simple terms to facilitate meaningful discussion between the business owners and engineering. For example, a scorecard metric for scalability might be color-coded in a simple way. Green means meeting the defined criteria, yellow means failing to meet the defined criteria but actively implementing a planned remediation, and red means failing to meet the defined criteria with no plan or action.

It's important to emphasize that these metrics should directly reflect business needs.

### Service-review phase

The service-review phase is the core of the operational fitness review. It involves these steps:

1. **Measure service metrics.** Use the scorecard metrics to monitor the services, to ensure that the services meet the business expectations. Service monitoring is essential. If you can't monitor a set of services with respect to the nonfunctional requirements, consider the corresponding scorecard metrics to be red. In this case, the first step for remediation is to implement the appropriate service monitoring. For example, if the business expects a service to operate with 99.99 percent availability, but there is no production telemetry in place to measure availability, assume that you're not meeting the requirement.
2. **Plan remediation.** For each service operation for which metrics fall below an acceptable threshold, determine the cost of remediating the service to bring operation to an acceptable level. If the cost of remediating the service is greater than the expected revenue generation of the service, move on to consider the intangible costs, such as customer experience. For example, if customers have difficulty placing a successful order by using the service, they might choose a competitor instead.
3. **Implement remediation.** After the business owners and engineering team agree on a plan, implement it. Report the status of the implementation whenever you review scorecard metrics.

This process is iterative, and ideally your enterprise has a team dedicated to it. This team should meet regularly to review existing remediation projects, kick off the fundamental review of new workloads, and track the enterprise's overall scorecard. The team should also have the authority to hold remediation teams accountable if they're behind schedule or fail to meet metrics.

## Structure of the review team

The team responsible for operational fitness review is composed of the following roles:

- **Business owner:** Provides knowledge of the business to identify and prioritize each mission-critical business operation. This role also compares the mitigation cost to the business impact, and drives the final decision on remediation.
- **Business advocate:** Breaks down business operations into discreet parts, and maps those parts to services and infrastructure, whether on-premises or in the cloud. The role requires deep knowledge of the technology associated with each business operation.
- **Engineering owner:** Implements the services associated with the business operation. These individuals might participate in the design, implementation, and deployment of any solutions for nonfunctional requirement problems that are uncovered by the review team.
- **Service owner:** Operates the business's applications and services. These individuals collect logging and usage data for these applications and services. This data is used both to identify problems and to verify fixes after they're deployed.

## Review meeting

We recommend that your review team meet on a regular basis. For example, the team might meet monthly, and then report status and metrics to senior leadership on a quarterly basis.

Adapt the details of the process and meeting to fit your specific needs. We recommend the following tasks as a starting point:

1. The business owner and business advocate enumerate and determine the nonfunctional requirements for each business operation, with input from the engineering and service owners. For business operations that have been identified previously, review and verify the priority. For new business operations, assign a priority in the existing list.
2. The engineering and service owners map the current state of business operations to the corresponding on-premises and cloud services. The mapping is a list of the components in each service, oriented as a dependency tree. The engineering and service owners then determine the critical paths through the tree.
3. The engineering and service owners review the current state of operational logging and monitoring for the services listed in the previous step. Robust logging and monitoring are critical: they identify service components that contribute to a failure to meet nonfunctional requirements. If sufficient logging and monitoring aren't in place, the team must put them in place by creating and implementing a plan.
4. The team creates scorecard metrics for new business operations. The scorecard consists of the list of constituent components for each service identified in step 2. It's aligned with the nonfunctional requirements, and includes a measure of how well each component meets the requirements.
5. For constituent components that fail to meet nonfunctional requirements, the team designs a high-level solution, and assigns an engineering owner. At this point, the business owner and business advocate establish a budget for the remediation work, based on the expected revenue of the business operation.
6. Finally, the team conducts a review of the ongoing remediation work. Each of the scorecard metrics for work in progress is reviewed against the expected criteria. For constituent components that meet metric criteria, the service owner presents logging and monitoring data to confirm that the criteria are met. For those constituent components that don't meet metric criteria, each engineering owner explains the problems that are preventing criteria from being met, and presents any new designs for remediation.

## Recommended resources

- [Microsoft Azure Well-Architected Framework](#): Learn about guiding tenets for improving the quality of a workload. The framework consists of five pillars of architecture excellence:
  - Cost optimization
  - Operational excellence
  - Performance efficiency
  - Reliability
  - Security
- [Ten design principles for Azure applications](#). Follow these design principles to make your application more scalable, resilient, and manageable.
- [Designing resilient applications for Azure](#). Build and maintain reliable systems using a structured approach over the lifetime of an application, from design and implementation to deployment and operations.
- [Cloud design patterns](#). Use design patterns to build applications on the pillars of architecture excellence.
- [Azure Advisor](#). Azure Advisor provides personalized recommendations based on your usage and configurations to help optimize your resources for high availability, security, performance, and cost.

# IT management and operations in the cloud

11/9/2020 • 2 minutes to read • [Edit Online](#)

As a business moves to a cloud-based model, the importance of proper management and operations can't be overstated. Unfortunately, few organizations are prepared for the IT management shift that's required for success in building a cloud-first operating model. This section of the Cloud Adoption Framework outlines the operating model, processes, and tooling that have proven successful in the cloud. Each of these areas represents a minor but fundamental change in the way the business should view IT operations and management as it begins to adopt the cloud.

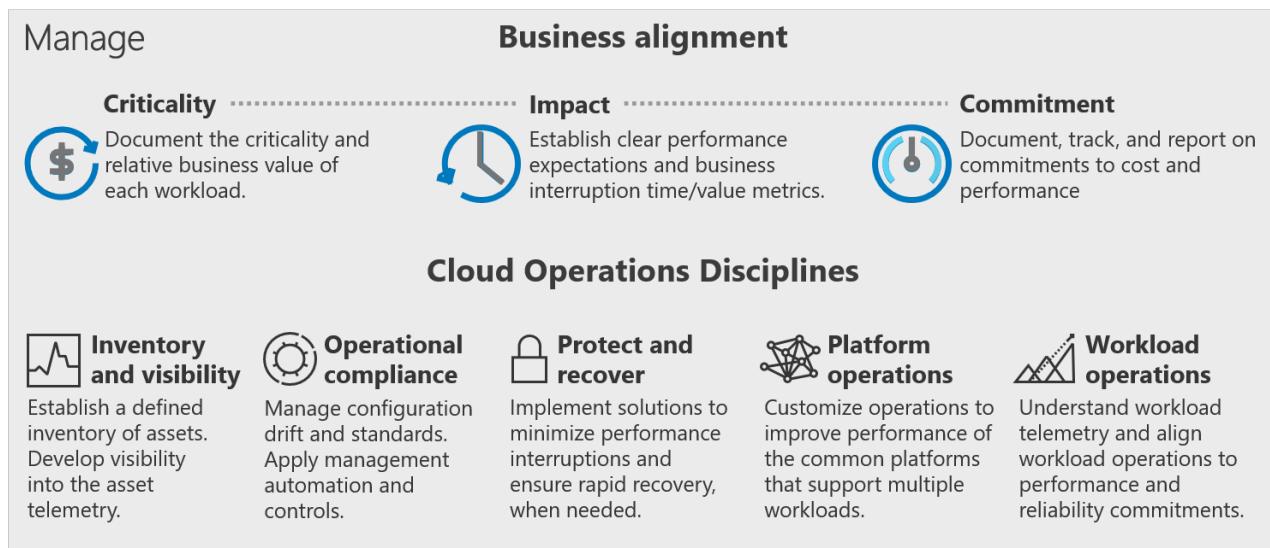
## Brief history of IT management

Before the cloud, IT management grew from a simple acquisition function. Acquisition of technical equipment to support business processes required technical expertise and deep experience with a specific group of equipment vendors. IT management consolidated the selection, acquisition, and configuration of IT assets. Generally, the acquired assets included storage, computing power, networking, and other similar assets that are required to power the desired business function. As the primary subject matter experts on the equipment, IT was also tasked with operating the equipment to ensure maximum performance and minimal business disruptions.

When the business builds out new technology solutions, it has a clear need that can justify the significant expenses associated with acquiring assets, or even building out full datacenters. When it builds solutions, the business sees the acquisition costs as an investment in the future. After the business need is met, the perception of the same costs shifts. Costs that are associated with existing solutions are seen as operational drag that's created by past needs. That perception is why many businesses view IT as a cost center. It's also why many IT organizations experience regular cost-control exercises or reductions in IT staff.

## Cloud management

The historical IT operating model was sufficient for over 20 years. But that model is now outdated and is less desirable than cloud-first alternatives. When IT management teams move to the cloud, they have an opportunity to rethink this model and drive greater value for the business. This article series outlines a modernized model of IT management.



## Next steps

For a deeper understanding of the new cloud management model, start with [Understand business alignment](#).

[Understand business alignment](#)

# Create business alignment in cloud management

11/9/2020 • 2 minutes to read • [Edit Online](#)

In on-premises environments, IT assets (applications, virtual machines, VM hosts, disk, servers, devices, and data sources) are managed by IT to support workload operations. In IT terms, a workload is a collection of IT assets that support a specific business operation. To help support business operations, IT management delivers processes that are designed to minimize disruptions to those assets. When an organization moves to the cloud, management and operations shift a bit, creating an opportunity to develop tighter business alignment.

## Business vernacular

The first step in creating business alignment is to ensure term alignment. IT management, like most engineering professions, has amassed a collection of jargon, or highly technical terms. Such terms can lead to confusion for business stakeholders and make it difficult to map management services to business value.

Fortunately, the process of developing a cloud adoption strategy and cloud adoption plan creates an ideal opportunity to remap these terms. The process also creates opportunities to rethink commitments to operational management, in partnership with the business. The following article series walks you through this new approach across three specific terms that can help improve conversations among business stakeholders:

- **Criticality:** Mapping workloads to business processes. Ranking criticality to focus investments.
- **Impact:** Understanding the impact of potential outages to aid in evaluating return on investment for cloud management.
- **Commitment:** Developing true partnerships, by creating and documenting agreements with the business.

### NOTE

Underlying these terms are classic IT terms such as SLA, RTO, and RPO. Mapping specific business and IT terms is covered in more detail in the [Commitment](#) article.

## Operations management workbook

To help capture decisions that result from this conversation about term alignment, an [operations management workbook](#) is available on our GitHub site. This workbook does not perform SLA or cost calculations. It serves only to help capture such measures and forecast return on loss-avoidance efforts.

Alternatively, these same workloads and associated assets could be tagged directly in Azure, if the solutions are already deployed to the cloud.

## Next steps

Start creating business alignment by defining [workload criticality](#).

[Define workload criticality](#)

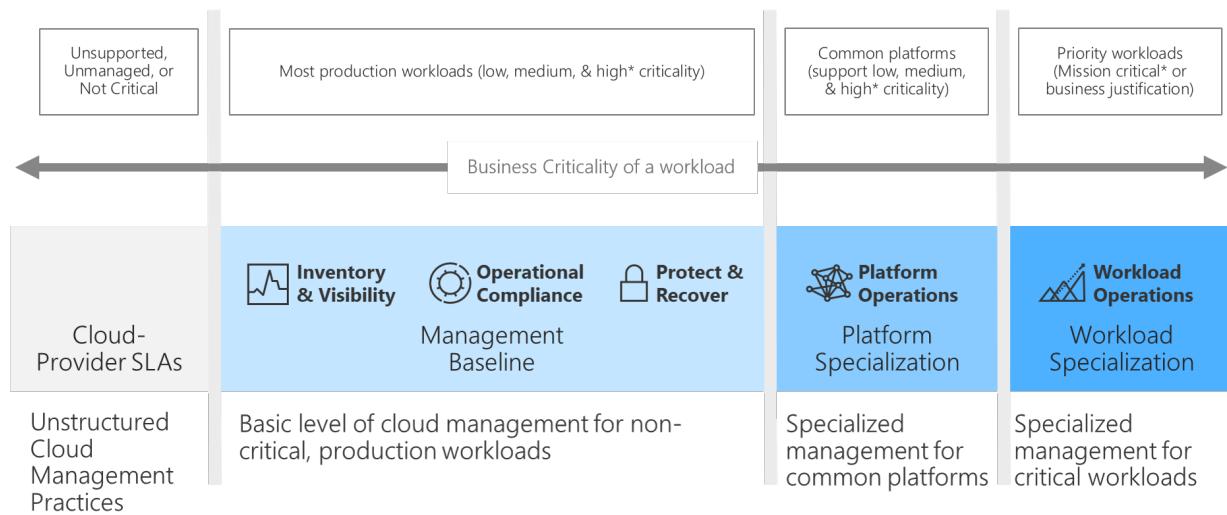
# Business criticality in cloud management

11/9/2020 • 3 minutes to read • [Edit Online](#)

Across every business, there exist a small number of workloads that are too important to fail. These workloads are considered mission critical. When those workloads experience outages or performance degradation, the adverse impact on revenue and profitability can be felt across the entire company.

At the other end of the spectrum, some workloads can go months at a time without being used. Poor performance or outages for those workloads is not desirable, but the impact is isolated and limited.

Understanding the criticality of each workload in the IT portfolio is the first step toward establishing mutual commitments to cloud management. The following diagram illustrates a common alignment between the criticality scale to follow and the standard commitments made by the business.



## Criticality scale

The first step in any business criticality alignment effort is to create a criticality scale. The following table presents a sample scale to be used as a reference, or template, for creating your own scale.

CRITICALITY	BUSINESS VIEW
Mission-critical	Affects the company's mission and might noticeably affect corporate profit-and-loss statements.
Unit-critical	Affects the mission of a specific business unit and its profit-and-loss statements.
High	Might not hinder the mission, but affects high-importance processes. Measurable losses can be quantified in the case of outages.
Medium	Impact on processes is likely. Losses are low or immeasurable, but brand damage or upstream losses are likely.
Low	Impact on business processes isn't measurable. Neither brand damage nor upstream losses are likely. Localized impact on a single team is likely.

CRITICALITY	BUSINESS VIEW
Unsupported	No business owner, team, or process that's associated with this workload can justify any investment in the ongoing management of the workload.

It's common for businesses to include additional criticality classifications that are specific to their industry, vertical, or specific business processes. Examples of additional classifications include:

- **Compliance-critical:** In heavily regulated industries, some workloads might be critical as part of an effort to maintain compliance requirements.
- **Security-critical:** Some workloads might not be mission critical, but outages could result in loss of data or unintended access to protected information.
- **Safety-critical:** When lives or the physical safety of employees and customers is at risk during an outage, it can be wise to classify workloads as safety-critical.

## Importance of accurate criticality

Later in the cloud-adoption process, the cloud management team will use this classification to determine the amount of effort required to meet aligned levels of criticality. In on-premises environments, operations management is often purchased centrally and treated as a necessary business burden, with little or no additional operating costs. Like all cloud services, operations management is purchased on a per-asset basis as monthly operating costs.

Because there's a clear and direct cost to operations management in the cloud, it's important to properly align costs and desired criticality scales.

## Select a default criticality

An initial review of every workload in the portfolio can be time consuming. To ensure that this effort doesn't block your broader cloud strategy, we recommend that your teams agree on a default criticality to apply to all workloads.

Based on the preceding criticality-scale table, we recommend that you adopt *medium* criticality as the default. Doing so will allow your cloud strategy team to quickly identify workloads that require a higher level of criticality.

## Use the template

The following steps apply if you're using the [operations management workbook](#) to plan for cloud management.

1. Record the criticality scale in the [Scale](#) worksheet.
2. Update each workload in either the [Example](#) worksheet or the [Clean Template](#) worksheet to reflect the default criticality in the [Criticality](#) column.
3. The business should enter the correct values to reflect any deviations from the default criticality.

## Next steps

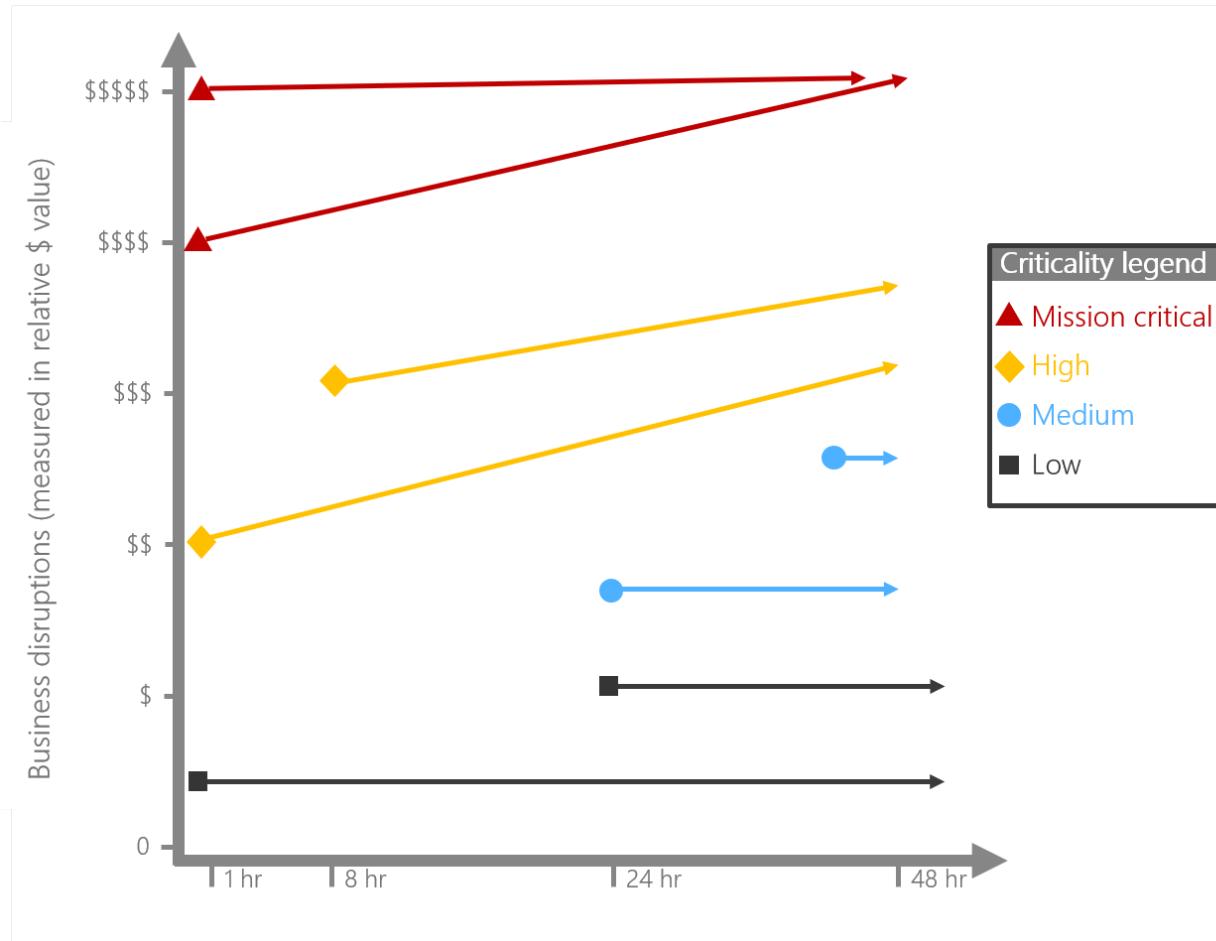
After your team has defined business criticality, you can [calculate and record business impact](#).

[Calculate and record business impact](#)

# Business impact in cloud management

5/22/2020 • 4 minutes to read • [Edit Online](#)

Assume the best, prepare for the worst. In IT management, it's safe to assume that the workloads required to support business operations will be available and will perform within agreed-upon constraints, based on the selected criticality. However, to manage investments wisely, it's important to understand the impact on the business when an outage or performance degradation occurs. This importance is illustrated in the following graph, which maps potential business interruptions of specific workloads to the business impact of outages across a relative value scale.



To create a fair basis of comparison for the impact on various workloads across a portfolio, a time/value metric is suggested. The time/value metric captures the adverse impact of a workload outage. Generally, this impact is recorded as a direct loss of revenue or operating revenue during a typical outage period. More specifically, it calculates the amount of lost revenue for a unit of time. The most common time/value metric is *Impact per hour*, which measures operating revenue losses per hour of outage.

A few approaches can be used to calculate impact. You can apply any of the options in the following sections to achieve similar outcomes. It's important to use the same approach for each workload when you calculate protected losses across a portfolio.

## Start with estimates

Current operating models might make it difficult to determine an accurate impact. Fortunately, few systems need a highly accurate loss calculation. In the previous step, *Classify Criticality*, we suggested that you start all workloads with a default of *medium criticality*. Medium criticality workloads generally receive a standard level of

management support with a relatively low impact on operating cost. Only when a workload requires additional operational management resources might you require an accurate financial impact.

For all standardized workloads, business impact serves as a prioritization variable when you're recovering systems during an outage. Outside of those limited situations, the business impact creates little to no change in the operations management experience.

## Calculate time

Depending on the nature of the workload, you could calculate losses differently. For high-paced transactional systems such as a real-time trading platform, losses per millisecond might be significant. Less frequently used systems, such as payroll, might not be used every hour. Whether the frequency of usage is high or low, it's important to normalize the time variable when you calculate financial impact.

## Calculate total impact

When you want to consider additional management investments, it's more important that the business impact be more accurate. The following three approaches to calculating losses are ordered from most accurate to least accurate:

- **Adjusted losses:** If your business has experienced a major loss event in the past, such as a hurricane or other natural disaster, a claims adjuster might have calculated actual losses during the outage. These calculations are based on insurance industry standards for loss calculation and risk management. Using adjusted losses as the total amount of losses in a specific time frame can lead to highly accurate projections.
- **Historical losses:** If your on-premises environment has suffered historically from outages resulting from infrastructure instability, it can be a bit harder to calculate losses. But you can still apply the adjuster formulas used internally. To calculate historical losses, compare the deltas in sales, gross revenue, and operating costs across three time frames: before, during, and after outage. By examining these deltas, you can identify accurate losses when no other data is available.
- **Complete loss calculation:** If no historical data is available, you can derive a comparative loss value. In this model, you determine the average gross revenue per hour for the business unit. When you're projecting loss avoidance investments, it's not fair to assume that a complete system outage equates to a 100 percent loss of revenue. But you can use this assumption as a rough basis for comparing loss impacts and prioritizing investments.

Before you make certain assumptions about potential losses associated with workload outages, it's a good idea to work with your finance department to determine the best approach to such calculations.

## Calculate workload impact

When you're calculating losses by applying historical data, you might have enough information to clearly determine the contribution of each workload to those losses. Performing this evaluation is where partnerships within the business are absolutely critical. After the total impact has been calculated, that impact must be attributed across each of the workloads. That distribution of impact should come from the business stakeholders, who should agree on the relative and cumulative impact of each workload. To that end, your team should solicit feedback from business executives to validate alignment. Such feedback is often equal parts emotion and subject matter expertise. It's important that this exercise represent the logic and beliefs of the business stakeholders who should have a say in budget allocation.

## Use the template

If you're using the [Operations Management workbook](#) to plan for cloud management, consider doing the following:

- Each business should update each workload in either the [Example](#) worksheet or the [Clean Template](#) worksheet, along with the [Time/Value Impact](#) of each workload. By default, [Time/Value Impact](#) represents the projected losses per hour associated with an outage of the workload.

## Next steps

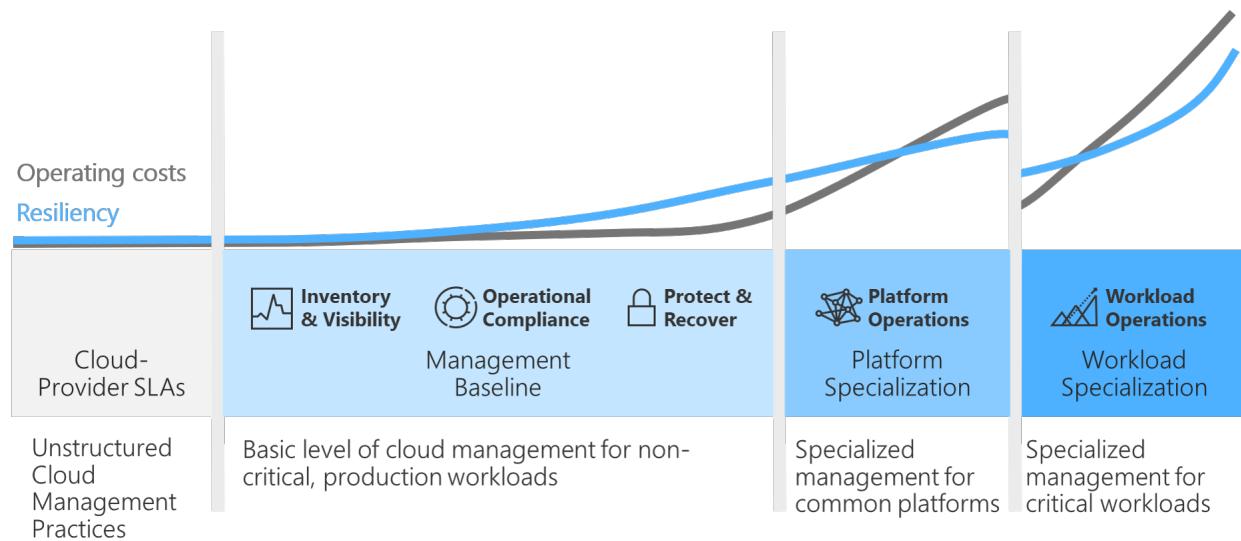
After the business has defined impact, you can [align commitments](#).

[Align management commitments with the business](#)

# Business commitment in cloud management

11/9/2020 • 9 minutes to read • [Edit Online](#)

Defining *business commitment* is an exercise in balancing priorities. The objective is to align the proper level of operational management at an acceptable operating cost. Finding that balance requires a few data points and calculations, which we've outlined in this article.



Commitments to business stability, via technical resiliency or other service-level agreement (SLA) impacts, are a business justification decision. For most workloads in an environment, a baseline level of cloud management is sufficient. For others, a 2x to 4x cost increase is easily justified because of the potential impact of any business interruptions.

The previous articles in this series can help you understand the classification and impact of interruptions to various workloads. This article helps you calculate the returns. As illustrated in the preceding image, each level of cloud management has inflection points where cost can rise faster than increases in resiliency. Those inflection points will prompt detailed business decisions and business commitments.

## Determine a proper commitment with the business

For each workload in the portfolio, the cloud operations team and cloud strategy team should align on the level of management that's provided directly by the cloud operations team.

As you're establishing a commitment with the business, there are a few key aspects to align:

- IT operations prerequisites.
- Management responsibility.
- Cloud tenancy.
- Soft-cost factors.
- Loss avoidance ROI.
- Validation of management level.

To aid in your decision process, the remainder of this article describes each of these aspects in greater detail.

## IT operations prerequisites

The [Azure Management Guide](#) outlines the management tools that are available in Azure. Before reaching a

commitment with the business, IT should determine an acceptable standard-level management baseline to be applied to all managed workloads. IT would then calculate a standard management cost for each of the managed workloads in the IT portfolio, based on counts of CPU cores, disk space, and other asset-related variables. IT would also estimate a composite SLA for each workload, based on the architecture.

#### TIP

IT operations teams often use a default minimum of 99.9 percent uptime for the initial composite SLA. They might also choose to normalize management costs based on the average workload, especially for solutions with minimal logging and storage needs. Averaging the costs of a few medium criticality workloads can provide a starting point for initial conversations.

#### TIP

If you're using the [operations management workbook](#) to plan for cloud management, the operations management fields should be updated to reflect these prerequisites. Those fields include *Commitment level*, *Composite SLA*, and *Monthly cost*. Monthly cost should represent the cost of the added operational management tools on a monthly basis.

The operations management baseline serves as an initial starting point to be validated in each of the following sections.

## Management responsibility

In a traditional on-premises environment, the cost of managing the environment is commonly assumed to be a sunk cost that's owned by IT operations. In the cloud, management is a purposeful decision with direct budgetary impact. The costs of each management function can be more directly attributed to each workload that's deployed to the cloud. This approach allows for greater control, but it does create a requirement for cloud operations teams and cloud strategy teams to first commit to an agreement about responsibilities.

Organizations might also choose to [outsource some of their ongoing management functions to a service provider](#). These service providers can use [Azure Lighthouse](#) to give organizations more precise control in granting access to their resources, along with greater visibility into the actions performed by the service providers.

- **Delegated responsibility:** Because there's no need to centralize and assume operational management overhead, IT operations for many organizations are considering new approaches. One common approach is referred to as *delegated responsibility*. In a cloud center of excellence model, platform operations and platform automation provide self-service management tools that can be used by business-led operations teams, independent of a centralized IT operations team. This approach gives business stakeholders complete control over management-related budgets. It also allows the cloud center of excellence (CCoE) team to ensure that a minimum set of guardrails has been properly implemented. In this model, IT acts as a broker and a guide to help the business make wise decisions. Business operations oversee day to day operations of dependent workloads.
- **Centralized responsibility:** Compliance requirements, technical complexity, and some shared service models might require a *Central IT team* model. In this model, IT continues to exercise its operations management responsibilities. Environmental design, management controls, and governance tooling might be centrally managed and controlled, which restricts the role of business stakeholders in making management commitments. But the visibility into the cost and architecture of cloud approaches makes it much easier for centralized IT to communicate the cost and level of management for each workload.
- **Mixed model:** Classification is at the heart of a *mixed model* of management responsibilities. Companies that are in the midst of a transformation from on-premises to cloud might require an on-premises-first operating model for a while. Companies with strict compliance requirements, or that depend on long-term

contracts with IT outsourcing vendors, might require a centralized operating model.

Regardless of their constraints, today's businesses must innovate. When rapid innovation must flourish, in the midst of a central-IT, centralized-responsibility model, a mixed-model approach might provide balance. In this approach, a central IT team provides a centralized operating model for all workloads that are mission-critical or contain sensitive information. At the same time, all other workload classifications might be placed in a cloud environment that's designed for delegated responsibilities. The centralized responsibility approach serves as the general operating model. The business then has flexibility to adopt a specialized operating model, based on its required level of support and sensitivity.

The first step is committing to a responsibility approach, which then shapes the following commitments.

**Which organization will be responsible for day-to-day operations management for this workload?**

## Cloud tenancy

For most businesses, management is easier when all assets reside in a single tenant. However, some organizations might need to maintain multiple tenants. To learn why a business might require a multitenant Azure environment, see [Centralize management operations with Azure Lighthouse](#).

**Will this workload reside in a single Azure tenant, alongside all other workloads?**

## Soft-cost factors

The next section outlines an approach to comparative returns that are associated with levels of management processes and tooling. At the end of that section, each analyzed workload measures the cost of management relative to the forecast impact of business disruptions. That approach provides a relatively easy way to understand whether an investment in richer management approaches is warranted.

Before you run the numbers, it's important to look at the soft-cost factors. Soft-cost factors produce a return, but that return is difficult to measure through direct hard-cost savings that would be visible in a profit-and-loss statement. Soft-cost factors are important because they can indicate a need to invest in a higher level of management than is fiscally prudent.

A few examples of soft-cost factors would include:

- Daily workload usage by the board or CEO.
- Workload usage by the top  $x\%$  of customers that leads to a greater revenue impact elsewhere.
- Impact on employee satisfaction.

The next data point that's required to make a commitment is a list of soft-cost factors. These factors don't need to be documented at this stage, but business stakeholders should be aware of the importance of these factors and their exclusion from the following calculations.

## Calculate loss avoidance ROI

When it's calculating the relative return on operations management costs, the IT team that's responsible for Cloud Operations should complete the previously mentioned prerequisites and assume a minimum level of management for all workloads.

The next commitment to be made is an acceptance by the business of the costs associated with the baseline-managed offering.

**Does the business agree to invest in the baseline offering to meet minimum standards of cloud operations?**

If the business does not agree to that level of management, a solution must be devised that allows the business to

proceed, without materially affecting the cloud operations of other workloads.

If the business wants more than the standard management level, the remainder of this section will help validate that investment and the associated returns (in the form of loss avoidance).

### **Increased levels of management: Design principles and service catalog**

For managed solutions, several design principles and template solutions can be applied in addition to the management baseline. Each of the design principles for reliability and resiliency adds operating cost to the workload. For IT and the business to agree on these additional commitments, it's important to understand potential losses that can be avoided through that increased investment.

The following calculations will walk through formulas to help you better understand the differences between losses and increased management investments. For guidance on calculating the cost of increased management, see [Workload automation](#) and [Platform automation](#).

#### **TIP**

If you're using the [operations management workbook](#) to plan for cloud management, update the operations management fields to reflect to reflect each conversation. Those fields include *Commitment level*, *Composite SLA*, and *Monthly cost*. Monthly cost should represent the monthly cost of the added operational management tools. After they're updated, the fields will update the ROI formulas and each of the following fields.

#### **Estimate outage (hours per year)**

Composite SLA is the service-level agreement that's based on the deployment of each asset in the workload. That field drives *estimated outage* (labeled `Est. Outage` in the workbook). To calculate estimated outage in hours per year without using the workbook, apply the following formula:

$$\text{Estimated outage} = (1 - \text{Composite SLA percentage}) \times \text{Number of hours in a year}$$

The workbook uses the default value of *8,760 hours per year*.

#### **Standard loss impact**

*Standard loss impact* (labeled `Standard Impact` in the workbook) forecasts the financial impact of any outage, assuming that the *estimated outage* prediction proves accurate. To calculate this forecast without using the workbook, apply the following formula:

$$\text{Standard impact} = \text{Estimated outage} @ \text{three 9s of uptime} \times \text{Time-value impact}$$

This serves as a baseline for cost, should the business stakeholders choose to invest in a higher level of management.

#### **Composite-SLA impact**

*Composite-SLA impact* (labeled `Commitment level impact` in the workbook) provides updated fiscal impact, based on the changes to the uptime SLA. This calculation allows you to compare the projected financial impact of both options. To calculate this forecast impact without the spreadsheet, apply the following formula:

$$\text{Composite-SLA impact} = \text{Estimated outage} \times \text{Time-value impact}$$

The value represents the potential losses to be avoided by the changed commitment level and new composite SLA.

#### **Comparison basis**

*Comparison basis* evaluates standard impact and composite SLA impact to determine which is most appropriate in the return column.

## Return on loss avoidance

If the cost of managing a workload exceeds the potential losses, the proposed investment in cloud management might not be fruitful. To compare the *Return on Loss Avoidance*, see the column labeled *Annual ROI*\*\*\*\*. To calculate this column on your own, use the following formula:

$$\text{Return on Loss Avoidance} = (\text{Comparison basis} - (\text{Monthly cost} \times 12)) \div (\text{Monthly cost} \times 12)$$

Unless there are other soft-cost factors to consider, this comparison can quickly suggest whether there should be a deeper investment in cloud operations, resiliency, reliability, or other areas.

## Validate the commitment

By this point in the process, commitments have been made: centralized or delegated responsibility, Azure tenancy, and level of commitment. Each commitment should be validated and documented to ensure that the cloud operations team, the cloud strategy team, and the business stakeholders are aligned on this commitment to manage the workload.

## Next steps

After the commitments are made, the responsible operations teams can begin configuring the workload in question. To get started, evaluate various approaches to [inventory and visibility](#).

[Inventory and visibility options](#)

# Management leveling across cloud management disciplines

11/9/2020 • 3 minutes to read • [Edit Online](#)

The keys to proper management in any environment are consistency and repeatable processes. There are endless of options for the things that can be done in Azure. Likewise, there are countless approaches to cloud management. To provide consistency and repeatability, it's important to narrow those options to a consistent set of management processes and tools that will be offered for workloads hosted in the cloud.

## Suggested management levels

Because the workloads in your IT portfolio vary, it's unlikely that a single level of management will suffice for each workload. To help you support a variety of workloads and business commitments, we suggest that your cloud operations team or platform operations team establish a few levels of operations management.



As a starting point, consider establishing the management levels that are shown in the preceding diagram and suggested in the following list:

- **Management baseline:** A cloud management baseline (or management baseline) is a defined set of tools, processes, and consistent pricing that serve as the foundation for all cloud management in Azure. To establish a cloud management baseline and determine which tools to include in the baseline offering to your business, review the list in the "Cloud management disciplines" section.
- **Enhanced baseline:** Some workloads might require enhancements to the baseline that aren't necessarily specific to a single platform or workload. Although these enhancements aren't cost effective for every workload, there should be common processes, tools, and solutions for any workload that can justify the cost of the extra management support.
- **Platform specialization:** In any given environment, some common platforms are used by a variety of workloads. This general architectural commonality doesn't change when businesses adopt the cloud. Platform specialization is an elevated level of management that applies data and architectural subject matter expertise to provide a higher level of operational management. Examples of platform specialization would include management functions specific to SQL Server, Containers, Active Directory, or other services that can be better managed through consistent, repeatable processes, tools, and architectures.
- **Workload specialization:** For workloads that are truly mission critical, there might be a cost justification to go much deeper into the management of that workload. Workload specialization applies workload telemetry to determine more advanced approaches to daily management. That same data often identifies automation, deployment, and design improvements that would lead to greater stability, reliability, and resiliency beyond what's possible with operational management alone.
- **Unsupported:** It's equally important to communicate common management processes that won't be delivered through cloud management disciplines for workloads that are classified as not supported or not critical.

Organizations might also choose to [outsource functions related to one or more of these management levels to a service provider](#). These service providers can use [Azure Lighthouse](#) to provide greater precision and transparency.

The remaining articles in this series outline processes that are commonly found within each of these disciplines. In parallel, the [Azure Management Guide](#) demonstrates the tools that can support each of those processes. For assistance with building your management baseline, start with the Azure Management Guide. After you've established the baseline, this article series and the accompanying best practices can help expand that baseline to define other levels of management support.

## Cloud management disciplines

Each suggested management level can call on a variety of cloud management disciplines. However, the mapping is designed to make it easier to find the suggested processes and tools to deliver on the appropriate level of cloud management.

In most cases, the previously discussed *management baseline level* consists of processes and tools from the following disciplines. In each case, a few processes and tools are highlighted to demonstrate *enhanced baseline functions*.

- **Inventory and visibility:** At a minimum, a management baseline should include a means of inventorying assets and creating visibility into the run state of each asset.
- **Operational compliance:** Regular management of configuration, sizing, cost, and performance of assets is key to maintaining performance expectations and a management baseline.
- **Protect and recover:** Minimizing operational interruptions and expediting recovery can help you avoid performance losses and revenue impacts. Detection and recovery are essential aspects of this discipline within any management baseline.

The platform specialization level of management pulls from the processes and tools that are aligned with the platform operations disciplines. Likewise, the workload specialization level of management pulls from the processes and tools that are aligned with the workload operations disciplines.

## Next steps

The next step toward defining each level of cloud management is an understanding of [inventory and visibility](#).

[Inventory and visibility options](#)

# Inventory and visibility in cloud management

11/9/2020 • 6 minutes to read • [Edit Online](#)

Operational management has a clear dependency on data. Consistent management requires an understanding about what is managed (inventory) and how those managed workloads and assets change over time (visibility). Clear insights about inventory and visibility help empower the team to manage the environment effectively. All other operational management activities and processes build on these two areas.

A few classic phrases about the importance of measurements set the tone for this article:

- Manage what matters.
- You can only manage what you can measure.
- If you can't measure it, it might not matter.

The inventory and visibility discipline builds on these timeless phrases. Before you can effectively establish operational management processes, it's important to gather data and create the right level of visibility for the right teams.

## Common customer challenges

Unless inventory and visibility processes are consistently applied, operational management teams can suffer from a higher volume of business interruptions, longer time to recovery, and greater amounts of effort required to troubleshoot and triage issues. As changes adversely affect higher priority applications and larger numbers of assets, each of these metrics grows even faster.

These challenges stem from a small number of questions that can be answered only through consistent data/telemetry:

- How does the current-state performance deviate from standard operational performance telemetry?
- What assets are causing the business interruptions at the workload level?
- Which assets must be remediated to return to acceptable performance of this workload or business process?
- When did the deviation start? What was the trigger?
- Which changes have been made to the underlying assets? By whom?
- Were the changes intentional? Malicious?
- How did changes affect performance telemetry?

It is difficult, if not impossible, to answer these questions without a rich, centralized source for logs and telemetry data. To enable cloud management by ensuring the consistent configuration that's required to centralize the data, the baseline service must first start by defining the processes. The processes should capture how such a configuration enforces data collection to support the components of inventory and visibility in the next section.

## Components of inventory and visibility

Creating visibility on any cloud platform requires a few key components:

- Responsibility and visibility
- Inventory
- Central logging
- Change tracking
- Performance telemetry

## **Responsibility and visibility**

When you establish commitments for each workload, [management responsibility](#) is a key factor. Delegated responsibility creates a need for delegated visibility. The first step toward inventory and visibility is to ensure that the responsible parties have access to the right data. Before you implement any cloud-native tools for visibility, ensure that each monitoring tool has been configured with proper access and scope for each operations team.

## **Inventory**

If no one knows that an asset exists, it's difficult to manage the asset. Before an asset or workload can be managed, it must be inventoried and classified. The first technical step toward stable operations is a validation of inventory and classification of that inventory.

## **Central logging**

Centralized logging is critical to the visibility that's required day to day by the operations management teams. All assets deployed to the cloud should record logs to a central location. In Azure, that central location is log analytics. The centralization of logging drives reports about change management, service health, configuration, and most other aspects of IT operations.

Enforcing the consistent use of central logging is the first step toward establishing repeatable operations. Enforcement can be accomplished through corporate policy. When possible, however, enforcement should be automated to ensure consistency.

## **Change tracking**

Change is the one constant in a technology environment. Awareness and understanding of changes across multiple workloads is essential to reliable operations. Any cloud management solution should include a means of understanding the when, how, and why of technical change. Without those data points, remediation efforts are significantly hindered.

## **Performance telemetry**

Business commitments about cloud management are driven by data. To properly maintain commitments, the cloud operations team must first understand the telemetry about the stability, performance, and operations of the workload, and the assets that support the workload.

The ongoing health and operations of the network, DNS, operating systems, and other foundational aspects of the environment are critical data points that factor into the overall health of any workload.

# **Processes**

Perhaps more important than the features of the cloud management platform, the cloud management processes will realize operations commitments with the business. Any cloud management methodology should include, at a minimum, the following processes:

- **Reactive monitoring:** When deviations adversely affect business operations, who addresses those deviations? What actions do they take to remediate the deviations?
- **Proactive monitoring:** When deviations are detected but business operations are not affected, how are those deviations addressed, and by whom?
- **Commitment reporting:** How is adherence to the business commitment communicated to business stakeholders?
- **Budgetary reviews:** What is the process for reviewing those commitments against budgeted costs? What is the process for adjusting the deployed solution or the commitments to create alignment?
- **Escalation paths:** What escalation paths are available when any of the preceding processes fail to meet the needs of the business?

There are several more processes related to inventory and visibility. The preceding list is designed to provoke thought within the operations team. Answering these questions will help develop some of the necessary

processes, as well as likely trigger new, deeper questions.

## Responsibilities

When you're developing processes for operational monitoring, it's equally important to determine responsibilities for daily operation and regular support of each process.

In a centralized IT organization, IT provides the operational expertise. The business would be consultative in nature, when issues require remediation.

In a cloud center of excellence organization, business operations would provide the expertise and hold responsibility for management of these processes. IT would focus on the automation and support of teams, as they operate the environment.

But these are the common responsibilities. Organizations often require a mixture of responsibilities to meet business commitments.

## Act on inventory and visibility

Regardless of the cloud platform, the five components of inventory and visibility are used to drive most operational processes. All subsequent disciplines will build on the data that's being captured. The next articles in this series outline ways to act on that data and integrate other data sources.

### Share visibility

Data without action produces little return. Cloud management might expand beyond cloud-native tools and processes. To accommodate broader processes, a cloud management baseline might need to be enhanced to include reporting, IT Service Management integration, or data centralization. Cloud management might need to include one or more of the following during various phases of operational maturity.

### Report

Offline processes and communication about commitments to business stakeholders often require reporting. Self-service reporting or periodic reporting might be a necessary component of an enhanced management baseline.

### IT service management (ITSM) integration

ITSM integration is often the first example of acting on inventory and visibility. When deviations from expected performance patterns arise, ITSM integration uses alerts from the cloud platform to trigger tickets in a separate IT service management tool to trigger remediation activities. Some operating models might require ITSM integration as an aspect of the enhanced management baseline.

### Data centralization

There's a variety of reasons why a business might require multiple tenants within a single cloud provider. In those scenarios, data centralization is a required component of the enhanced management baseline, because it can provide visibility across each of those tenants or environments.

## Next steps

Operational compliance builds on inventory capabilities by applying management automation and controls. See how [operational compliance](#) maps to your processes.

[Plan for operational compliance](#)

# Operational compliance in cloud management

5/12/2020 • 2 minutes to read • [Edit Online](#)

Operational compliance builds on the discipline of [inventory and visibility](#). As the first actionable step of cloud management, this discipline focuses on regular telemetry reviews and remediation efforts (both proactive and reactive remediation). This discipline is the cornerstone for maintaining balance between security, governance, performance, and cost.

## Components of operations compliance

Maintaining compliance with operational commitments requires analysis, automation, and human remediation. Effective operational compliance requires consistency in a few critical processes:

- Resource consistency
- Environment consistency
- Resource configuration consistency
- Update consistency
- Remediation automation

### Resource consistency

The most effective step that a cloud management team can take toward operational compliance is to establish consistency in resource organization and tagging. When resources are consistently organized and tagged, all other operational tasks become easier. For deeper guidance on resource consistency, see the [Governance methodology](#). Specifically, review the [initial governance foundation articles](#) to learn how to start developing resource consistency.

### Environment consistency

Establishing consistent environments, or landing zones, is the next most important step toward operational compliance. When landing zones are consistent and enforced through automated tools, it is significantly less complex to diagnose and resolve operational issues. For deeper guidance on environment consistency, see the [Ready phase](#) of the cloud adoption lifecycle. The exercises in that phase help build a repeatable process for defining and maturing a consistent, code-first approach to the development of cloud-based environments.

### Resource configuration consistency

As it builds on governance and readiness approaches, cloud management should include processes for the ongoing monitoring and evaluation of its adherence to resource consistency requirements. As workloads change or new versions are adopted, it is vital that cloud management processes evaluate any configuration changes, which are not easily regulated through automation.

When inconsistencies are discovered, some are addressed by consistency in updates and others can be automatically remediated.

### Update consistency

Stability in approach can lead to more stable operations. But some changes are required within cloud management processes. In particular, regular patching and performance changes are essential to reducing interruptions and controlling costs.

One of the many values of a mature cloud management methodology is a focus on stabilizing and controlling necessary change.

Any cloud management baseline should include a means of scheduling, controlling, and possibly automating

necessary updates. Those updates should include patches at a minimum, but could also include performance, sizing, and other aspects of updating assets.

### **Remediation automation**

As an enhanced baseline for cloud management, some workloads may benefit from automated remediation. When a workload commonly encounters issues that can't be resolved through code or architectural changes, automating remediation can help reduce the burden of cloud management and increase user satisfaction.

Many would argue that any issue that's common enough to automate should be resolved through resolution of technical debt. When a long-term resolution is prudent, it should be the default option. However, some business scenarios make it difficult to justify large investments in the resolution of technical debt. When such a resolution can't be justified, but remediation is a common and costly burden, automated remediation is the next best solution.

## Next steps

[Protection and recovery](#) are the next areas to consider in a cloud management baseline.

[Protect and recover](#)

# Protect and recover in cloud management

11/9/2020 • 5 minutes to read • [Edit Online](#)

After they've met the requirements for [inventory and visibility](#) and [operational compliance](#), cloud management teams can anticipate and prepare for a potential workload outage. As they're planning for cloud management, the teams must start with an assumption that something will fail.

No technical solution can consistently offer a 100 percent uptime SLA. Solutions with the most redundant architectures claim to deliver on "six 9s" or 99.9999 percent uptime. But even a "six 9s" solution goes down for 31.6 seconds in any given year. Sadly, it's rare for a solution to warrant a large, ongoing operational investment that's required to reach "six 9s" of uptime.

Preparation for an outage allows the team to detect failures sooner and recover more quickly. The focus of this discipline is on the steps that come immediately after a system fails. How do you protect workloads, so that they can be recovered quickly when an outage occurs?

## Translate protection and recovery conversations

The workloads that power business operations consist of applications, data, virtual machines (VMs), and other assets. Each of those assets might require a different approach to protection and recovery. The important aspect of this discipline is to establish a consistent commitment within the management baseline, which can provide a starting point during business discussions.

At a minimum, each asset that supports any given workload should have a baseline approach with a clear commitment to speed of recovery (recovery time objectives, or RTO) and risk of data loss (recovery point objectives, or RPO).

### **Recovery time objectives (RTO)**

When disaster strikes, a recovery time objective is the amount of time it should take to recover any system to its state prior to the disaster. For each workload, that would include the time required to restore minimum necessary functionality for the VMs and apps. It also includes the amount of time required to restore the data that's required by the applications.

In business terms, RTO represents the amount of time that the business process will be out of service. For mission-critical workloads, this variable should be relatively low, allowing the business processes to resume quickly. For lower-priority workloads, a standard level of RTO might not have a noticeable impact on company performance.

The management baseline should establish a standard RTO for non-mission-critical workloads. The business can then use that baseline as a way to justify additional investments in recovery times.

### **Recovery point objectives (RPO)**

In most cloud management systems, data is periodically captured and stored through some form of data protection. The last time data was captured is referred to as a recovery point. When a system fails, it can be restored only to the most recent recovery point.

If a system has a recovery point objective that's measured in hours or days, a system failure would result in the loss of data for those hours or days between the last recovery point and the outage. A one-day RPO would theoretically result in the loss of all transactions in the day leading up to the failure.

For mission-critical systems, an RPO that's measured in minutes or seconds might be more appropriate to use to avoid a loss in revenue. But a shorter RPO generally results in an increase in overall management costs.

To help minimize costs, a management baseline should focus on the longest acceptable RPO. The cloud

management team can then increase the RPO of specific platforms or workloads, which would warrant more investment.

## Protect and recover workloads

Most of the workloads in an IT environment support a specific business or technical process. Systems that don't have a systemic impact on business operations often don't warrant the increased investments required to recover quickly or minimize data loss. By establishing a baseline, the business can clearly understand what level of recovery support can be offered at a consistent, manageable price point. This understanding helps the business stakeholders evaluate the value of an increased investment in recovery.

For most cloud management teams, an enhanced baseline with specific RPO/RTO commitments for various assets yields the most favorable path to mutual business commitments. The following sections outline a few common enhanced baselines that empower the business to easily add protection and recovery functionality through a repeatable process.

### Protect and recover data

Data is arguably the most valuable asset in the digital economy. The ability to protect and recover data more effectively is the most common enhanced baseline. For the data that powers a production workload, loss of data can be directly equated to loss in revenue or loss of profitability. We generally encourage cloud management teams to offer a level of enhanced management baseline that supports common data platforms.

Before cloud management teams implement platform operations, it's common for them to support improved operations for a platform as a service (PaaS) data platform. For instance, it's easy for a cloud management team to enforce a higher frequency of backup or multiregion replication for Azure SQL Database or Azure Cosmos DB solutions. Doing so allows the development team to easily improve RPO by modernizing their data platforms.

To learn more about this thought process, see [platform operations discipline](#).

### Protect and recover VMs

Most workloads have some dependency on virtual machines, which host various aspects of the solution. For the workload to support a business process after a system failure, some virtual machines must be recovered quickly.

Every minute of downtime on those virtual machines could cause lost revenue or reduced profitability. When VM downtime has a direct impact on the fiscal performance of the business, RTO is very important. Virtual machines can be recovered more quickly by using replication to a secondary site and automated recovery, a model that's referred to as a hot-warm recovery model. At the highest state of recovery, virtual machines can be replicated to a fully functional, secondary site. This more expensive approach is referred to as a high-availability, or hot-hot, recovery model.

Each of the preceding models reduces the RTO, resulting in a faster restoration of business process capabilities. However, each model also results in significantly increased cloud management costs.

Also, please note that, apart from replication for high-availability, backup should be enabled for scenarios such as accidental delete, data corruption and ransomware attacks.

For more information about this thought process, see [workload operations discipline](#).

## Next steps

After this management baseline component is met, the team can look ahead to avoid outages in its [platform operations](#) and [workload operations](#).

# Platform operations in cloud management

11/9/2020 • 6 minutes to read • [Edit Online](#)

A cloud management baseline that spans [inventory and visibility](#), [operational compliance](#), and [protection and recovery](#) might provide a sufficient level of cloud management for most workloads in the IT portfolio. However, that baseline is seldom enough to support the full portfolio. This article builds on the most common next step in cloud management, portfolio operations.

A quick study of the assets in the IT portfolio highlights patterns across the workloads that are being supported. Within those workloads, there will be common platforms. Depending on the past technical decisions within the company, those platforms could vary widely.

For some organizations, there will be a heavy dependence on SQL Server, Oracle, or other open-source data platforms. In other organizations, the commonalities might be rooted in the hosting platforms for virtual machines (VMs) or containers. Still others might have a common dependency on applications or Enterprise Resource Planning (ERP) systems, such as SAP, Oracle, or others.

By understanding these commonalities, the cloud management team can specialize in higher levels of support for those prioritized platforms.

## Establish a service catalog

The objective of platform operations is to create reliable and repeatable solutions, which the cloud adoption team can use to deliver a platform that provides a higher level of business commitment. That commitment could decrease the likelihood or frequency of downtime, which improves reliability. In the event of a system failure, the commitment could also help decrease the amount of data loss or time to recovery. Such a commitment often includes ongoing, centralized operations to support the platform.

As the cloud management team establishes higher degrees of operational management and specialization related to specific platforms, those platforms are added to a growing service catalog. The service catalog provides self-service deployment of platforms in a specific configuration, which adheres to ongoing platform operations. During the business-alignment conversation, cloud management and cloud strategy teams can propose service catalog solutions as a way for the business to improve reliability, uptime, and recovery commitments in a controlled, repeatable process.

For reference, some organizations refer to an early-stage service catalog as an *approved list*. The primary difference is that a service catalog comes with ongoing operational commitments from the cloud center of excellence (CCoE). An approved list is similar, in that it provides a preapproved list of solutions that a team can use in the cloud. However, typically there isn't an operational benefit associated with applications on an approved list.

Much like the debate between centralized IT and CCoE, the difference is one of priorities. A service catalog assumes good intent but provides operational, governance, and security guardrails that accelerate innovation. An approved list hinders innovation until operations, compliance, and security gates can be passed for a solution. Both solutions are viable, but they require the company to make subtle prioritization decisions to invest more in innovation or compliance.

### Build the service catalog

Cloud management is seldom successful at delivering a service catalog in a silo. Proper development of the catalog requires a partnership across the central IT team or the CCoE. This approach tends to be most successful when an IT organization reaches a CCoE level of maturity, but could be implemented sooner.

When it's building the service catalog within a CCoE model, the cloud platform team builds out the desired-state

platform. The cloud governance and cloud security teams validate governance and compliance within the deployment. The cloud management team establishes ongoing operations for that platform. And the cloud automation team packages the platform for scalable, repeatable deployment.

After the platform is packaged, the cloud management team can add it to the growing service catalog. From there, the cloud adoption team can use the package or others in the catalog during deployment. After the solution goes to production, the business realizes the extra benefits of improved operational management and potentially reduced business disruptions.

#### **NOTE**

Building a service catalog requires a great deal of effort and time from multiple teams. Using the service catalog or approved list as a gating mechanism will slow innovation. When innovation is a priority, service catalogs should be developed parallel to other adoption efforts.

## Define your own platform operations

Although management tools and processes can help improve platform operations, that is often not enough to achieve the desired states of stability and reliability. True platform operations requires a focus on pillars of architecture excellence. When a platform justifies a deeper investment in operations, consider the following five pillars before the platform becomes a part of any service catalog:

- **Cost optimization:** Manage costs to maximize the value delivered.
- **Operational excellence:** Follow operational processes that keep a system running in production.
- **Performance efficiency:** Scale systems to adapt to changes in load.
- **Reliability:** Design systems to recover from failures and continue to function.
- **Security:** Protect applications and data from threats.

The [Microsoft Azure Well-Architected Framework](#) provides an approach to evaluating specific workloads for adherence to these pillars, in an effort to improve overall operations. These pillars can be applied to both platform operations and workload operations.

## Get started with specific platforms

The platforms discussed in the next sections are common to typical Azure customers, and they can easily justify an investment in platform operations. Cloud management teams tend to start with them when they're building out platform operations requirements or a full service catalog.

### **PaaS data operations**

Data is often the first platform to warrant platform operations investments. When data is hosted in a platform as a service (PaaS) environment, business stakeholders tend to request a reduced recovery point objective (RPO) to minimize data loss. Depending on the nature of the application, they might also request a reduction in recovery time objective (RTO). In either case, the architecture that supports PaaS-based data solutions can easily accommodate some increased level of management support.

In most scenarios, the cost of improving management commitments is easily justified, even for applications that are not mission critical. This platform operations improvement is so common that many cloud management teams see it more as an enhanced baseline, rather than as a true platform operations improvement.

### **IaaS data operations**

When data is hosted in a traditional infrastructure as a service (IaaS) solution, the effort to improve RPO and RTO can be significantly higher. Yet the business stakeholders' desire to achieve better management commitments is seldom affected by a PaaS versus IaaS decision. If anything, an understanding of the fundamental differences in architecture might prompt the business to ask for PaaS solutions or commitments that match what's available on

PaaS solutions. Modernization of any IaaS data platforms should be considered as a first step into platform operations.

When modernization isn't an option, cloud management teams commonly prioritize IaaS-based data platforms as a first required service in the service catalog. Providing the business with a choice between standalone data servers and clustered, high-availability, data solutions makes the business commitment conversation much easier to facilitate. A basic understanding of the operational improvements and the increased costs will arm the business to make the best decision for the business processes and supporting workloads.

### **Other common platform operations**

In addition to data platforms, virtual machine hosts tend to be a common platform for operations improvements. Most commonly, cloud platform and cloud management teams invest in improvements to VMware hosts or container solutions. Such investments can improve the stability and reliability of the hosts, which support the VMs, which in turn power the workloads. Proper operations on one host or container can improve the RPO or RTO of several workloads. This approach creates improved business commitments, but distributes the investment. Improved commitments and reduced costs combine to make it much easier to justify improvements to cloud management and platform operations.

## Next steps

In parallel with improvements to platform operations, cloud management teams also focus on improving [workload operations](#) for the top 20 percent or less of production workloads.

### [Improve workload operations](#)

# Workload operations in cloud management

11/9/2020 • 5 minutes to read • [Edit Online](#)

Some workloads are critical to the success of the business. For those workloads, a management baseline is insufficient to meet the required business commitments to cloud management. Platform operations might not even be sufficient to meet business commitments. This highly important subset of workloads requires a specialized focus on the way the workload functions and how it is supported.

In return, the investment in workload operations can lead to improved performance, decreased risk of business interruption, and faster recovery when system failures occur. This article discusses an approach to investing in the continued operations of these high priority workloads to drive improved business commitments.

## When to invest in workload operations

The *Pareto principle* (also known as the *80/20 rule*) states that 80 percent of effects come from 20 percent of the causes. When IT portfolios are allowed to grow organically over time, this rule is often illustrated in a review of the IT portfolio. Depending on the effect that requires investment, the cause can vary but the general principle holds true:

- 80 percent of system failures tend to be the result of 20 percent of the common errors or bugs.
- 80 percent of business value tends to come from 20 percent of the workloads in a portfolio.
- 80 percent of the effort to migrate to the cloud comes from 20 percent of the workloads being moved.
- 80 percent of cloud management efforts will support 20 percent of the service incidents or trouble tickets.
- 80 percent of business impact from an outage will come from 20 percent of the systems affected by the outage.

Workload operations should be applied only when the cloud adoption strategy, business outcomes, and operational metrics are each well understood. This is a paradigm shift from the classic view of IT. Traditionally, IT assumed that all workloads experienced the same degree of support and required similar levels of priority.

Before they invest in deep workload operations, both IT and the business should understand the business justifications and the expectations of increased investment in cloud management.

## Start with the data

Workload operations begin with a deep understanding of workload performance and support requirements. Before the team invests in workload operations, it must have rich data about workload dependencies, application performance, database diagnostics, virtual machine telemetry, and incident history.

This data seeds the insights that drive workload operations decisions.

## Continued observation

Initial data and ongoing telemetry can help formulate and test theories about the performance of a workload. But ongoing workload operations are rooted in a continued and expanded observation of workload performance, with a heavy focus on application and data performance.

### Test the automation

At the application level, the first requirements of workload operations, is an investment in deep testing. For any application that's supported through workload operations, a test plan should be established and regularly executed to deliver functional and scale testing across the applications.

Regular test telemetry can provide immediate validation of various hypotheses about the operation of the workload. Improving operational and architectural patterns can be executed and tested. The resulting deltas provide a clear impact analysis to guide continued investments.

### **Understand releases**

A clear understanding of release cycles and release pipelines is an important element of workload operations.

An understanding of cycles can prepare for potential interruptions and allow the team to proactively address any releases that might produce an adverse effect on operations. This understanding also allows the cloud management team to partner with adoption teams to continuously improve the quality of the product and address any bugs that might affect stability.

More importantly, an understanding of release pipelines can significantly improve the recovery point objective (RPO) of a workload. In many scenarios, the fastest and most accurate path to the recovery of an application is a release pipeline. For application layers that change only when a new release happens, it might be wise to invest more heavily in pipeline optimization than on the recovery of the application from traditional back-up processes.

Although a deployment pipeline can be the fastest path to recovery, it can also be the fastest path to remediation. When an application has a fast, efficient, and reliable release pipeline, the cloud management team has an option to automate deployment to a new host as a form of automated remediation.

There might be many other faster, more effective mechanisms for remediation and recovery. However, when the use of an existing pipeline can meet business commitments and capitalize on existing DevOps investments, the existing pipeline might be a viable alternative.

### **Clearly communicate changes to the workload**

Change to any workload is among the biggest risks to workload operations. For any workload in the workload operations level of cloud management, the cloud management team should closely align with the cloud adoption teams to understand the changes coming from each release. This investment in proactive understanding will have a direct, positive impact on operational stability.

## **Improve outcomes**

The data and communication investments in a workload will yield suggestions for improvements to ongoing operations in one of three areas:

- Technical debt resolution
- Automated remediation
- Improved system design

### **Technical debt resolution**

The best workload operations plans still require remediation. As your cloud management team seeks to stay connected to understand adoption efforts and releases, the team likewise should regularly share remediation requirements to ensure that technical debt and bugs are a continued priority for your development teams.

### **Automated remediation**

By applying the Pareto principle, we can say that 80 percent of negative business impact likely comes from 20 percent of the service incidents. When those incidents can't be addressed in normal development cycles, investments in remediation automation can significantly reduce business interruptions.

### **Improved system design**

In the cases of technical debt resolution and automated remediation, system flaws are the common cause of most system outages. You can have the greatest impact on overall workload operations by adhering to a few design principles:

- **Scalability:** The ability of a system to handle increased load.

- **Availability:** The percentage of time that a system is functional and working.
- **Resiliency:** The ability of a system to recover from failures and continue to function.
- **Management:** Operations processes that keep a system running in production.
- **Security:** Protecting applications and data from threats.

To help improve overall operations, the [Microsoft Azure Well-Architected Framework](#) provides an approach to evaluating specific workloads for adherence to these pillars. Apply the pillars to both platform operations and workload operations.

## Next steps

With a full understanding of the manage methodology within the Cloud Adoption Framework, you are now armed to implement cloud management principles. Learn how to make this methodology actionable within your operations environment.

[Apply this methodology](#)

# Apply design principles and advanced operations

11/9/2020 • 6 minutes to read • [Edit Online](#)

The first three cloud management disciplines describe a management baseline. At a minimum, a management baseline should include a standard business commitment to minimize business interruptions and accelerate recovery if service is interrupted. Most management baselines include a disciplined focus on maintaining "inventory and visibility," "operational compliance," and "protection and recovery."

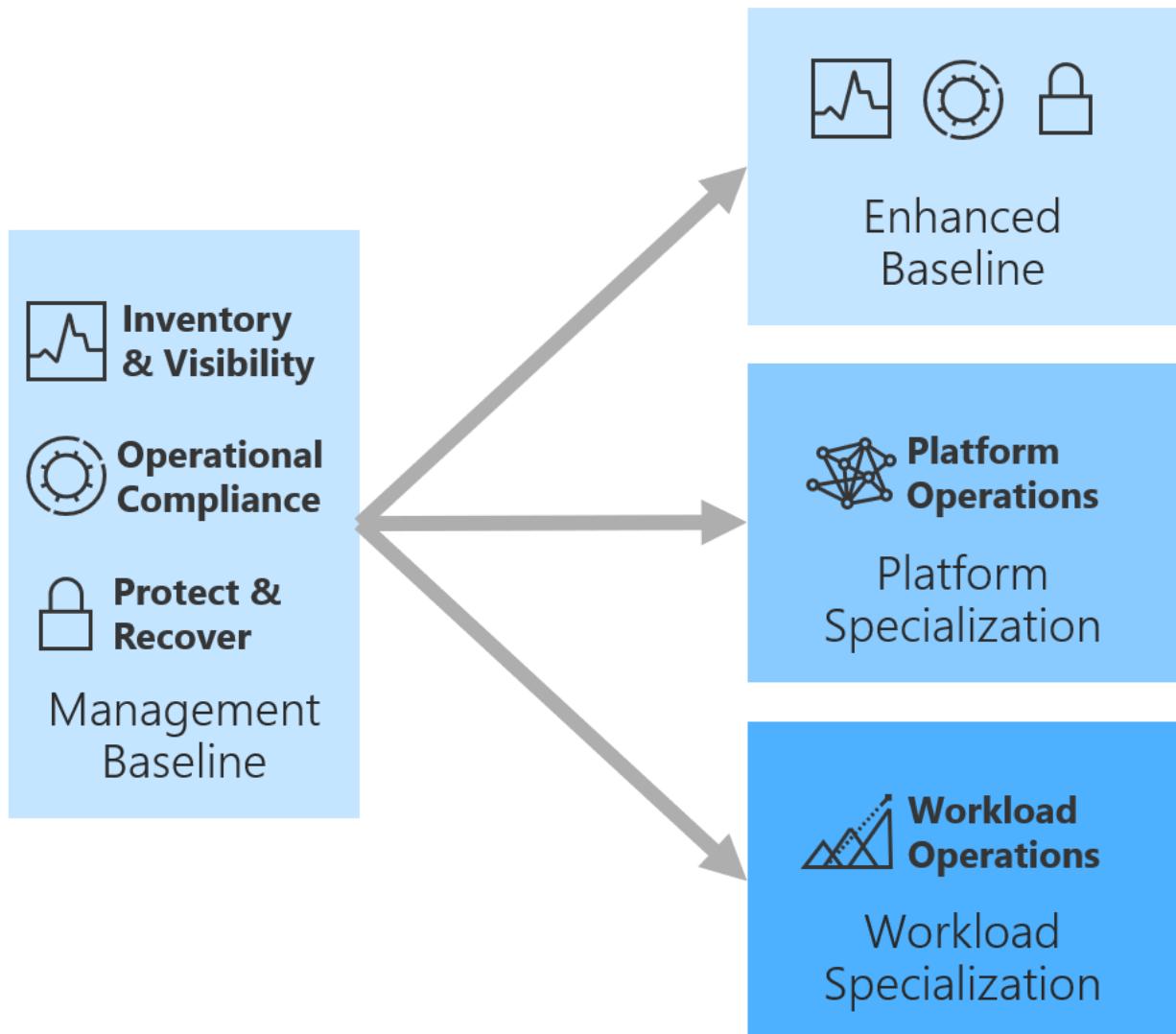
The purpose of a management baseline is to create a consistent offering that provides a minimum level of business commitment for all supported workloads. This baseline of common, repeatable management offerings allows the team to deliver a highly optimized degree of operational management, with minimal deviation. But that standard offering might not provide a rich enough commitment to the business.

The diagram in the next section illustrates three ways to go beyond the management baseline.

The management baseline should meet the minimum commitment required by 80 percent of the lowest criticality workloads in the portfolio. The baseline should not be applied to mission-critical workloads. Nor should it be applied to common platforms that are shared across workloads. Those workloads require a focus on design principles and advanced operations.

## Advanced operations options

There are three suggested paths for improving business commitments beyond the management baseline, as shown in the following diagram:



## Enhanced management baseline

As outlined in the Azure Management Guide, an enhanced management baseline uses cloud-native tools to improve uptime and decrease recovery times. The improvements are significant, but less so than with workload or platform specialization. The advantage of an enhanced management baseline is the equally significant reduction in cost and implementation time.

## Management specialization

Aspects of workload and platform operations might require changes to design and architecture principles. Those changes could take time and might result in increased operating expenses. To reduce the number of workloads requiring such investments, an enhanced management baseline could provide enough of an improvement to the business commitment.

For workloads that warrant a higher investment to meet a business commitment, specialization of operations is key.

## Areas of management specialization

There are two areas of specialization:

- **Platform specialization:** Invest in ongoing operations of a shared platform, distributing the investment across multiple workloads.
- **Workload specialization:** Invest in ongoing operations of a specific workload, generally reserved for

mission-critical workloads.

### Central IT team or cloud center of excellence (CCoE)

Decisions between platform specialization and workload specialization are based on the criticality and impact of each workload. However, these decisions are also indicative of larger cultural decisions between central IT team and CCoE organizational models.

Workload specialization often triggers a cultural change. Traditional IT and centralized IT both build processes that can provide support at scale. Scale support is more achievable for repeatable services found in a management baseline, enhanced baseline, or even platform operations. Workload specialization doesn't often scale. This lack of scale makes it difficult for a centralized IT organization to provide necessary support without reaching organizational scale limitations.

Alternatively, a cloud center of excellence approach scales through purposeful delegation of responsibility and selective centralization. Workload specialization tends to better align with the delegated responsibility approach of a CCoE.

The natural alignment of roles in a CCoE is outlined as follows:

- The cloud platform team helps build common platforms that support multiple cloud adoption teams.
- The cloud automation team extends those platforms into deployable assets in a service catalog.
- Cloud management delivers the management baseline centrally and helps support the use of the service catalog.
- But the business unit (in the form of a business DevOps team or cloud adoption team) holds responsibility for day-to-day operations of the workload, pipeline, or performance.

As for aligning areas of management, central IT team and CCoE models can generally deliver on Platform Specialization, with minimal cultural change. Delivering on workload specialization might be more complex for central IT teams.

## Management specialization processes

Within each specialization, the following four-step process is delivered in a disciplined, iterative approach. This approach requires partnership among cloud adoption, cloud platform, cloud automation, and cloud management experts to create a viable and informed feedback loop.

- **Improve system design:** Improve the design of common systems (platforms) or specific workloads to effectively minimize interruptions.
- **Automate remediation:** Some improvements are not cost effective. In such cases, it might make more sense to automate remediation and reduce the impact of interruptions.
- **Scale the solution:** As systems design and automated remediation are improved, you can scale those changes across the environment through the service catalog.
- **Continuous improvement:** You can use various monitoring tools to discover incremental improvements to address in the next pass of system design, automation, and scale.

### Improve system design

Improving system design is the most effective approach to improving operations of any common platform. System design improvements can help increase stability and decrease business interruptions. Design of individual systems is out of scope for the environment view taken throughout the Cloud Adoption Framework.

As a complement to this framework, the [Microsoft Azure Well-Architected Framework](#) provides guiding tenets for improving the quality of a platform or a specific workload. The framework focuses on improvement across five pillars of architecture excellence:

- **Cost optimization:** Manage costs to maximize the value delivered.

- **Operational excellence:** Follow operational processes that keep a system running in production.
- **Performance efficiency:** Scale systems to adapt to changes in load.
- **Reliability:** Design systems to recover from failures and continue to function.
- **Security:** Protect applications and data from threats.

Most business interruptions equate to some form of technical debt, or deficiency in the architecture. For existing deployments, systems design improvements can be viewed as payments against existing technical debt. For new deployments, systems design improvements can be viewed as avoidance of technical debt. The next section, "Automated remediation," looks at ways to address technical debt that can't or shouldn't be addressed.

To improve system design, learn more about the [Microsoft Azure Well-Architected Framework](#). As your system design improves, return to this article to find new opportunities to improve and scale the improvements across your environment.

### Automated remediation

Some technical debt can't or shouldn't be addressed. Resolution could be too expensive to correct. It could be planned but might have a long project duration. The business interruption might not have a significant business impact, or the business priority is to recover quickly instead of investing in resiliency.

When resolution of technical debt isn't the desired path, automated remediation is commonly the desired next step. Using Azure Automation and Azure Monitor to detect trends and provide automated remediation is the most common approach to automated remediation.

For guidance on automated remediation, see [Azure Automation and alerts](#).

### Scale the solution with a service catalog

The cornerstone of platform specialization and platform operations is a well-managed service catalog. This is how improvements to systems design and remediation are scaled across an environment. The cloud platform team and cloud automation team align to create repeatable solutions to the most common platforms in any environment. However, if those solutions aren't consistently applied, cloud management can provide little more than a baseline offering.

To maximize adoption and minimize maintenance overhead of any optimized platform, the platform should be added to a service catalog. Each application in the catalog can be deployed for internal consumption via the service catalog, or as a marketplace offering for external consumers.

For information about publishing to a service catalog, see the series on [publishing to a service catalog](#).

### Continuous improvement

Platform specialization and platform operations both depend on strong feedback loops between adoption, platform, automation, and management teams. Grounding those feedback loops in data empowers each team to make wise decisions. For platform operations to achieve long-term business commitments, it's important to take advantage of insights that are specific to the centralized platform. Because containers and SQL Server are the two most common centrally managed platforms, consider beginning with continuous improvement data collection by reviewing the following articles:

- [Container performance](#)
- [PaaS database performance](#)
- [IaaS database performance](#)

# Manage organizational alignment

11/9/2020 • 2 minutes to read • [Edit Online](#)

Cloud adoption can't happen without well-organized people. Successful cloud adoption is the result of properly skilled people doing the appropriate types of work, in alignment with clearly defined business goals, and in a well-managed environment. To deliver an effective operating model for the cloud, it's important to establish appropriately staffed organizational structures. This article outlines an approach to establishing and maintaining the proper organizational structures in four steps.

The following exercises will help guide the process of creating a landing zone to support cloud adoption.

1	<p><b>Structure type:</b> Define the type of organizational structure that best fits your operating model.</p>
2	<p><b>Cloud functions:</b> Understand the cloud functionality required to adopt and operate the cloud.</p>
3	<p><b>Mature team structures:</b> Define the teams that can provide various cloud functions.</p>
4	<p><b>RACI matrix:</b> Clearly defined roles are an important aspect of any operating model. Use the provided RACI matrix to map responsibility, accountability, consulted, and informed roles to each of the teams for various functions of the cloud operating model.</p>

## Structure type

The following organizational structures do not necessarily have to map to an organizational chart (org chart). Org charts generally reflect command and control management structures. Conversely, the following organizational structures are designed to capture alignment of roles and responsibilities. In an agile, matrix organization, these structures may be best represented as virtual teams. There is no limitation suggesting that these organizational structures couldn't be represented in an org chart, but it is not necessary in order to produce an effective operating model.

The first step of managing organizational alignment is to determine how the following organizational structures will be fulfilled:

- **Org chart alignment:** Management hierarchies, manager responsibilities, and staff alignment will align to organizational structures.
- **Virtual teams:** Management structures and org charts remain unchanged. Instead, virtual teams will be

created and tasked with the required functions.

- **Mixed model:** More commonly, a mixture of org chart and virtual team alignment will be required to deliver on transformation goals.

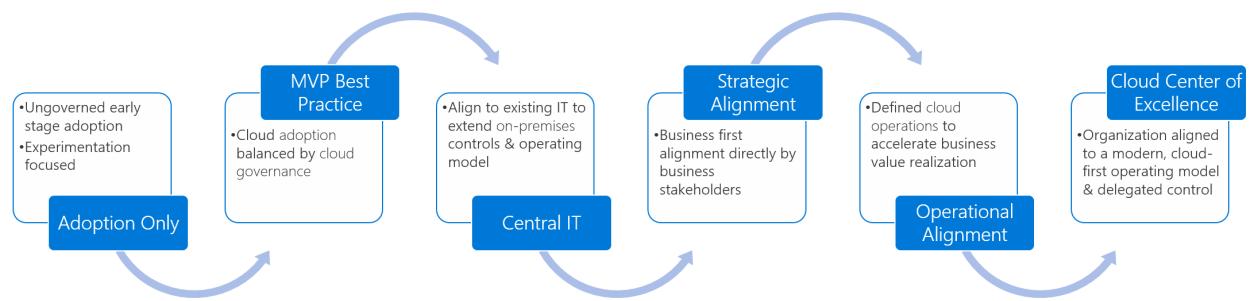
## Understand required cloud functions

The following is a list of functions that are required to succeed at cloud adoption and longer-term operating models. After you become familiar with these, they can be aligned to organizational structures based on staffing and maturity:

- **Cloud strategy:** Align technical change to business needs.
- **Cloud adoption:** Deliver technical solutions.
- **Cloud governance:** Manage risk.
- **Central IT team:** Support from existing IT staff.
- **Cloud operations:** Support and operate adopted solutions.
- **Cloud center of excellence:** Improve quality, speed, and resiliency of adoption.
- **Cloud platform:** Operate and mature the platform.
- **Cloud automation:** Accelerate adoption and innovation.
- **Cloud security:** Manage information security risk.

To some degree, each of these functions are delivered in every cloud adoption effort, either explicitly or in accordance with a defined team structure.

As adoption needs grow, so does the need to create balance and structure. To meet those needs, companies often follow a process of maturing organizational structures.



The article on [determining organizational structure maturity](#) provides additional detail regarding each level of maturity.

To track organization structure decisions over time, download and modify the [RACI template](#).

# Cloud strategy functions

11/9/2020 • 3 minutes to read • [Edit Online](#)

A cloud strategy team defines motivations and business outcomes, and validates and maintains alignment between business priorities and cloud adoption efforts. In the absence of a defined cloud strategy team, someone must still provide the functionality that aligns technical activities to business outcomes. That same person or group should also manage change across the project.

Cloud strategy functions are commonly provided by the following types of roles. When a cloud strategy team is defined, it should include many of the following roles:

- Finance
- Line of business
- Human resources
- Operations
- Enterprise architecture
- IT infrastructure
- Application groups
- Project managers (often with agile project management experience)

This helps guide critical prioritization and discovery efforts during cloud adoption. It may also trigger changes in business processes, the execution of operations, customer interactions, or even product development. If these functions are confined to IT, the success of cloud adoption efforts will be constrained. To drive true business change, business leaders should be the primary source of this functionality. A defined cloud strategy team provides a means for involving key participants in a structured way.

## NOTE

The organization's CEO and CIO often assign the team. Assignments are typically based on empowering this team to drive change that cuts across various different organizations within the enterprise. The cloud strategy team members should be assigned based on the [motivations for cloud adoption](#), [business outcomes](#), and relevant [financial models](#).

## Preparation

- [Learn the business value of Microsoft Azure](#).
- [Learn how the Cloud Adoption Framework](#) can help you align the strategy for business, people, and technology.
- Review the [cloud adoption strategy](#) process.
- Download the [strategy and plan template](#).

## Minimum scope

Align business stakeholders to maximize the business value of cloud adoption investments.

Whenever possible, business outcomes and the cloud strategy should both be defined early in the process. As investments in cloud adoption grows and business values are realized, business stakeholders often become more engaged. When cloud adoption efforts are led by the business, the focus might be on an operating model and the organization.

## **Establish a vision**

- [Adoption motivations](#): Document and articulate the reasons behind the technical effort.
- [Business outcomes](#): Clearly articulate what's expected of the technical team in terms of business changes.
- [Learning metrics](#): Establish short-term metrics that can show progress toward longer-term business outcomes.

## **Build business justification**

- [Cloud migration business case](#). Establish a business case for cloud migration.

## **Rationalize the digital estate**

- [Incremental rationalization](#): An agile approach to rationalization that properly aligns late-bound technical decisions.
- [The five Rs of rationalization](#): Understand the various rationalization options.

# **Deliverable**

The cloud strategy team drives critical prioritization and discovery efforts during cloud adoption. They may also change business processes, the execution of operations, customer interactions, or even product development. The primary focus of the cloud strategy team is to validate and maintain alignment between business priorities and cloud adoption efforts. Secondarily, this team should focus on change management across the adoption efforts. The cloud strategy team should be capable of delivering on the following tasks.

### **Early planning tasks:**

- Review and provide feedback on business outcomes and financial models.
- Aid in establishing clear motivations for cloud adoption that align with corporate objectives.
- Define relevant learning metrics that clearly communicate progress toward business outcomes.
- Understand business risks introduced by the plan, represent the business's tolerance for risk.
- Review and approve the rationalization of the digital estate.

### **Ongoing monthly tasks:**

- Support the cloud governance team during risk/tolerance conversations.
- Review release plans to understand timelines and business impact of technical change.
- Define business change plans associated with planned releases.
- Ensure business teams are ready to execute business testing and the business change plan.

### **Meeting cadence:**

Cloud strategy team members must be able to allocate time to planning and developing the cloud strategy:

- During early planning efforts, allocate an hour each week to meet with the team. After the adoption plan is solidified (usually within 4-6 weeks), the time requirements can be reduced.
- Throughout the adoption efforts, allocate 1-2 hours each month to review progress and validate continued priorities.
- Additional time is likely required from delegated members of the executive's team on an as-needed basis. Each member of the cloud strategy team should appoint a delegate who can allocate 5-10 hours per week to support ongoing prioritization questions and report on any urgent needs.

# **Next steps**

- Start a [cloud strategy team](#)
- Align your strategy with the [cloud adoption functions](#) by creating a [cloud adoption team](#) to work with.
- Use the [RACI template](#) to align responsibilities across teams.



# Cloud adoption functions

11/9/2020 • 3 minutes to read • [Edit Online](#)

Cloud adoption functions enable the implementation of technical solutions in the cloud. Like any IT project, the people delivering the actual work will determine success. The teams providing the necessary cloud adoption functions can be staffed from multiple subject matter experts or implementation partners.

Cloud adoption teams are the modern-day equivalent of technical implementation teams or project teams. But the nature of the cloud may require a more fluid team structure. Some teams focus exclusively on cloud migration, while other teams focus on innovations that take advantage of cloud technologies. Some teams include the broad technical expertise required to complete large adoption efforts, like a full datacenter migration. Other teams have a tighter technical focus and may move between projects to accomplish specific goals. One example would be a team of data platform specialists who help convert SQL VMs to SQL PaaS instances.

Regardless of the type or number of cloud adoption teams, the functionality required for cloud adoption is provided by subject matter experts found in IT, business analysis, or implementation partners.

Depending on the desired business outcomes, the skills needed to provide full cloud adoption functions could include:

- Infrastructure implementers
- DevOps engineers
- Application developers
- Data scientists
- Data or application platform specialists

For optimal collaboration and efficiency, we recommend that cloud adoption teams have an average team size of six people. These teams should be self-organizing from a technical execution perspective. We highly recommend that these teams also include project management expertise, with deep experience in agile, scrum, or other iterative models. This team is most effective when managed using a flat structure.

## Preparation

- [Create an Azure account](#): The first step to using Azure is to create an account.
- [Azure portal](#): Tour the Azure portal features and services, and customize the portal.
- [Introduction to Azure](#): Get started with Azure. Create and configure your first virtual machine in the cloud.
- [Azure fundamentals](#): Learn cloud concepts, understand the benefits, compare and contrast basic strategies, and explore the breadth of services available in Azure.
- Review the [Migrate methodology](#).

## Minimum scope

The nucleus of all cloud adoption efforts is the cloud migration team. This team drives the technical changes that enable adoption. Depending on the objectives of the adoption effort, this team may include a diverse range of team members who handle a broad set of technical and business tasks.

At a minimum, the team scope includes:

- [Rationalization of the digital estate](#)
- Review, validation, and advancement of the [prioritized migration backlog](#)

- The execution of the [first workload](#) as a learning opportunity.

## Deliverable

The primary need from any cloud adoption function is the timely, high-quality implementation of the technical solutions outlined in the adoption plan. These solutions should align with governance requirements and business outcomes, and should take advantage of technology, tools, and automation solutions that are available to the team.

### Early planning tasks:

- Execute the [rationalization of the digital estate](#).
- Review, validate, and advance the [prioritized migration backlog](#).
- Begin execution of the [first workload](#) as a learning opportunity.

### Ongoing monthly tasks:

- Oversee [change management processes](#).
- Manage the [release and sprint backlogs](#).
- Build and maintain the adoption landing zone in conjunction with governance requirements.
- Execute the technical tasks outlined in the [sprint backlogs](#).

### Meeting cadence:

We recommend that teams providing cloud adoption functions be dedicated to the effort full-time.

It's best if these teams meet daily in a self-organizing way. The goal of daily meetings is to quickly update the backlog, and to communicate what has been completed, what is to be done today, and what things are blocked, requiring additional external support.

Release schedules and iteration durations are unique to each company. But a range of one to four weeks per iteration seems to be the average duration. Regardless of iteration or release cadence, we recommend that the team meets all supporting teams at the end of each release to communicate the outcome of the release, and to reprioritize upcoming efforts. Likewise, it's valuable to meet as a team at the end of each sprint, with the cloud center of excellence or cloud governance team to stay aligned on common efforts and any needs for support.

Some of the technical tasks associated with cloud adoption can become repetitive. Team members should rotate every 3–6 months to avoid employee satisfaction issues and maintain relevant skills. A rotating seat on a cloud center of excellence or cloud governance team can provide an excellent opportunity to keep employees fresh and harness new innovations.

Learn more about the function of a [cloud center of excellence](#) or [cloud governance team](#).

## Next steps

- [Build a cloud adoption team](#)
- Align cloud adoption efforts with [cloud governance functions](#) to accelerate adoption and implement best practices, while reducing business and technical risks.

# Cloud governance functions

11/9/2020 • 7 minutes to read • [Edit Online](#)

A cloud governance team ensure that risks and risk tolerance are properly evaluated and managed. This team ensures the proper identification of risks that can't be tolerated by the business. The people on this team convert risks into governing corporate policies.

Depending on the desired business outcomes, the skills needed to provide full cloud governance functions include:

- IT governance
- Enterprise architecture
- Security
- IT operations
- IT infrastructure
- Networking
- Identity
- Virtualization
- Business continuity and disaster recovery
- Application owners within IT
- Finance owners

These baseline functions help you identify risks related to current and future releases. These efforts help you evaluate risk, understand the potential impacts, and make decisions regarding risk tolerance. When doing so, quickly update plans to reflect the changing needs of the [cloud migration team](#).

## Preparation

- Review the [Govern methodology](#).
- Take the [governance benchmark assessment](#).
- [Introduction to security in Azure](#): Learn the basic concepts to protect your infrastructure and data in the cloud. Understand what responsibilities are yours and what Azure handles for you.
- Understand how to work across groups to [manage cost](#).

## Minimum scope

- Understand [business risks](#) introduced by the plan.
- Represent the [business's tolerance for risk](#).
- Help create a [governance MVP](#).

Involve the following participants in cloud governance activities:

- Leaders from middle management and direct contributors in key roles should represent the business and help evaluate risk tolerances.
- The cloud governance functions are delivered by an extension of the [cloud strategy team](#). Just as the CIO and business leaders are expected to participate in cloud strategy functions, their direct reports are expected to participate in cloud governance activities.
- Business employees that are members of the business unit who work closely with the leadership of the line-of-business should be empowered to make decisions regarding corporate and technical risk.

- Information technology (IT) and information security (IS) employees who understand the technical aspects of the cloud transformation may serve in a rotating capacity instead of being a consistent provider of cloud governance functions.

## Deliverable

The cloud governance mission is to balance competing forces of transformation and risk mitigation. Additionally, cloud governance ensures that the [cloud migration team](#) is aware of data and asset classification, as well as architecture guidelines that govern adoption. Governance teams or individuals also work with the [cloud center of excellence](#) to apply automated approaches to governing cloud environments.

### Ongoing monthly tasks:

- Understand [business risks](#) introduced during each release.
- Represent the [business's tolerance for risk](#).
- Aid in the incremental improvement of [policy and compliance requirements](#).

### Meeting cadence:

The time commitment from each team member of the cloud governance team will represent a large percentage of their daily schedules. Contributions will not be limited to meetings and feedback cycles.

## Out of scope

As adoption scales, the cloud governance team may struggle to keep pace with innovations. This is especially true if your environment has heavy compliance, operations, or security requirements. If this happens you can shift some responsibilities to an existing IT team to reduce scope for the governance team.

## Next steps

Some large organizations have dedicated teams that focus on IT governance. These teams specialize in risk management across the IT portfolio. When those teams exist, the following maturity models can be accelerated quickly. But the IT governance team is encouraged to review the cloud governance model to understand how governance shifts slightly in the cloud. Key articles include extending corporate policy to the cloud and the Five Disciplines of Cloud Governance. No governance: It is common for organizations to move into the cloud with no clear plans for governance. Before long, concerns around security, cost, scale, and operations begin to trigger conversations about the need for a governance model and people to staff the processes associated with that model. Starting those conversations before they become concerns is always a good first step to overcome the antipattern of "no governance." The section on defining corporate policy can help facilitate those conversations.

**Governance blocked:** When concerns around security, cost, scale, and operations go unanswered, projects and business goals tend to get blocked. Lack of proper governance generates fear, uncertainty, and doubt among stakeholders and engineers. Stop this in its tracks by taking action early. The two governance guides defined in the Cloud Adoption Framework can help you start small, set initially limiting policies to minimize uncertainty and mature governance over time. Choose from the complex enterprise guide or standard enterprise guide.

**Voluntary governance:** There tend to be brave souls in every enterprise. Those gallant few who are willing to jump in and help the team learn from their mistakes. Often this is how governance starts, especially in smaller companies. These brave souls volunteer time to fix some issues and push cloud adoption teams toward a consistent well-managed set of best practices.

The efforts of these individuals are much better than "no governance" or "governance blocked" scenarios. While their efforts should be commended, this approach should not be confused with governance. Proper

governance requires more than sporadic support to drive consistency, which is the goal of any good governance approach. The guidance in the Five Disciplines of Cloud Governance can help develop this discipline.

**Cloud custodian:** This moniker has become a badge of honor for many cloud architects who specialize in early stage governance. When governance practices first start out, the results appear similar to those of governance volunteers. But there is one fundamental difference. A cloud custodian has a plan in mind. At this stage of maturity, the team is spending time cleaning up the messes made by the cloud architects who came before them. But the cloud custodian aligns that effort to well structured corporate policy. They also use governance governance tools, like those outlined in the governance MVP.

Another fundamental difference between a cloud custodian and a governance volunteer is leadership support. The volunteer puts in extra hours above regular expectations because of their quest to learn and do. The cloud custodian gets support from leadership to reduce their daily duties to ensure regular allocations of time can be invested in improving cloud governance.

**Cloud guardian:** As governance practices solidify and become accepted by cloud adoption teams, the role of cloud architects who specialize in governance changes a bit, as does the role of the cloud governance team. Generally, the more mature practices gain the attention of other subject matter experts who can help strengthen the protections provided by governance implementations.

While the difference is subtle, it is an important distinction when building a governance-focused IT culture. A cloud custodian cleans up the messes made by innovative cloud architects, and the two roles have natural friction and opposing objectives. A cloud guardian helps keep the cloud safe, so other cloud architects can move more quickly with fewer messes. Cloud guardians begin using more advanced governance approaches to accelerate platform deployment and help teams self-service their environmental needs, so they can move faster. Examples of these more advanced functions are seen in the incremental improvements to the governance MVP, such as improvement of the security baseline.

**Cloud accelerators:** Cloud guardians and cloud custodians naturally harvest scripts and governance tools that accelerate the deployment of environments, platforms, or even components of various applications. Curating and sharing these scripts in addition to centralized governance responsibilities develops a high degree of respect for these architects throughout IT.

Those governance practitioners who openly share their curated scripts help deliver technology projects faster and embed governance into the architecture of the workloads. This workload influence and support of good design patterns elevate cloud accelerators to a higher rank of governance specialist.

**Global governance:** When organizations depend on globally dispersed IT needs, there can be significant deviations in operations and governance in various geographies. Business unit demands and even local data sovereignty requirements can cause governance best practices to interfere with required operations. In these scenarios, a tiered governance model allows for minimally viable consistency and localized governance. The article on multiple layers of governance provides more insights on reaching this level of maturity.

Every company is unique, and so are their governance needs. Choose the level of maturity that fits your organization and use the Cloud Adoption Framework to guide the practices, processes, and tooling to help you get there.

As cloud governance matures, teams are empowered to adopt the cloud at faster paces. Continued cloud adoption efforts tend to trigger maturity in IT operations. Either develop a cloud operations team, or sync with your cloud operations team to ensure governance is a part of operations development.

Learn more about starting a [cloud governance team](#) or a [cloud operations team](#).

After you've established an [initial cloud governance foundation](#), use these best practices in [Governance foundation improvements](#) to get ahead of your adoption plan and prevent risks.

# Central IT team functions

11/9/2020 • 7 minutes to read • [Edit Online](#)

As cloud adoption scales, cloud governance functions alone may not be sufficient to govern adoption efforts. When adoption is gradual, teams tend to organically develop the skills and processes needed to be ready for the cloud over time.

But when one cloud adoption team uses the cloud to achieve a high-profile business outcome, gradual adoption is seldom the case. Success follows success. This is also true for cloud adoption, but it happens at cloud scale. When cloud adoption expands from one team to multiple teams relatively quickly, additional support from existing IT staff is needed. But those staff members may lack the training and experience required to support the cloud using cloud-native IT tools. This often drives the formation of a Central IT team governing the cloud.

**Caution**

While this is a common maturity step, it can present a high risk to adoption, potentially blocking innovation and migration efforts if not managed effectively. See the risk section below to learn how to mitigate the risk of centralization becoming a cultural antipattern.

The skills needed to provide centralized IT functions could be provided by:

- An existing Central IT team
- Enterprise architects
- IT operations
- IT governance
- IT infrastructure
- Networking
- Identity
- Virtualization
- Business continuity and disaster recovery
- Application owners within IT

**WARNING**

Centralized IT should only be applied in the cloud when existing delivery on-premises is based on a Central IT team model. If the current on-premises model is based on delegated control, consider a cloud center of excellence (CCoE) approach for a more cloud-compatible alternative.

## Key responsibilities

Adapt existing IT practices to ensure adoption efforts result in well-governed, well-managed environments in the cloud.

The following tasks are typically executed regularly:

### Strategic tasks

- Review:
  - **Business outcomes.**
  - **Financial models.**
  - **Motivations for cloud adoption.**

- Business risks.
- Rationalization of the digital estate.
- Monitor adoption plans and progress against the [prioritized migration backlog](#).
- Identify and prioritize platform changes that are required to support the migration backlog.
- Act as an intermediary or translation layer between cloud adoption needs and existing IT teams.
- Take advantage of existing IT teams to accelerate platform functions and enable adoption.

### **Technical tasks**

- Build and maintain the cloud platform to support solutions.
- Define and implement the platform architecture.
- Operate and manage the cloud platform.
- Continuously improve the platform.
- Keep up with new innovations in the cloud platform.
- Deliver new cloud functionality to support business value creation.
- Suggest self-service solutions.
- Ensure that solutions meet existing governance and compliance requirements.
- Create and validate deployment of platform architecture.
- Review release plans for sources of new platform requirements.

## Meeting cadence

Central IT team expertise usually comes from a working team. Expect participants to commit much of their daily schedules to alignment efforts. Contributions aren't limited to meetings and feedback cycles.

## Central IT team risks

Each of the cloud functions and phases of organizational maturity are prefixed with the word "cloud". The central IT team is the only exception. Centralized IT became prevalent when all IT assets could be housed in few locations, managed by a small number of teams, and controlled through a single operations management platform. Global business practices and the digital economy have largely reduced the instances of those centrally managed environments.

In the modern view of IT, assets are globally distributed. Responsibilities are delegated. Operations management is delivered by a mixture of internal staff, managed service providers, and cloud providers. In the digital economy, IT management practices are transitioning to a model of self-service and delegated control with clear guardrails to enforce governance. A central IT team can be a valuable contributor to cloud adoption by becoming a cloud broker and a partner for innovation and business agility.

A central IT team is well positioned to take valuable knowledge and practices from existing on-premises models and apply those practices to cloud delivery. But this process requires change. New processes, new skills, and new tools are required to support cloud adoption at scale. When a Central IT team adapts, it becomes an important partner in cloud adoption efforts. But if the Central IT team doesn't adapt to the cloud, or attempts to use the cloud as a catalyst for tight-grain controls, it quickly becomes a blocker to adoption, innovation, and migration.

The measures of this risk are speed and flexibility. The cloud simplifies adopting new technologies quickly. When new cloud functionality can be deployed within minutes, but the reviews by the Central IT team add weeks or months to the deployment process, then these centralized processes become a major impediment to business success. When this indicator is encountered, consider alternative strategies to IT delivery.

### **Exceptions**

Many industries require rigid adherence to third-party compliance. Some compliance requirements still demand centralized IT control. Delivering on these compliance measures can add time to deployment processes,

especially for new technologies that haven't been used broadly. In these scenarios, expect delays in deployment during the early stages of adoption. Similar situations may exist for companies that deal with sensitive customer data, but may not be governed by a third-party compliance requirement.

### **Operate within the exceptions**

When centralized IT processes are required and those processes create appropriate checkpoints in adoption of new technologies, these innovation checkpoints can still be addressed quickly. Governance and compliance requirements are designed to protect those things that are sensitive, not to protect everything. The cloud provides simple mechanisms for acquiring and deploying isolated resources while maintaining proper guardrails.

A mature Central IT team maintains necessary protections but negotiates practices that still enable innovation. Demonstrating this level of maturity depends on proper classification and isolation of resources.

### **Example narrative of operating within exceptions to empower adoption**

This example narrative illustrates the approach taken by a mature Central IT team at the fictional company Contoso to empower adoption.

Contoso has adopted a central IT team model for the support of the business's cloud resources. To deliver this model, they have implemented tight controls for various shared services such as ingress network connections. This wise move reduced the exposure of their cloud environment and provided a single "break-glass" device to block all traffic if a breach occurs. Their Security Baseline policies state that all ingress traffic must come through a shared device managed by the Central IT team.

But one of their cloud adoption teams now requires an environment with a dedicated and specially configured ingress network connection to use a specific cloud technology. An immature Central IT team would simply refuse the request and prioritize its existing processes over adoption needs. Contoso's Central IT team is different. They quickly identified a simple four-part solution to this dilemma:

1. **Classification:** Since the cloud adoption team was in the early stages of building a new solution and didn't have any sensitive data or mission-critical support needs, the assets in the environment were classified as low risk and noncritical. Effective classification is a sign of maturity in a central IT team. Classifying all assets and environments allows for clearer policies.
2. **Negotiation:** Classification alone isn't sufficient. Shared services were implemented to consistently operate sensitive and mission-critical assets. Changing the rules would compromise governance and compliance policies designed for the assets that need more protection. Empowering adoption can't happen at the cost of stability, security, or governance. This led to a negotiation with the adoption team to answer specific questions. Could a business-led DevOps team provide operations management for this environment? Would this solution require direct access to other internal resources? If the cloud adoption team is comfortable with those tradeoffs, then the ingress traffic might be possible.
3. **Isolation:** Since the business can provide its own ongoing operations management, and since the solution doesn't rely on direct traffic to other internal assets, it can be cordoned off in a new subscription. That subscription is also added to a separate node of the new management group hierarchy.
4. **Automation:** Another sign of maturity in this team is their automation principles. The team uses Azure Policy to automate policy enforcement. They also use Azure Blueprints to automate deployment of common platform components and enforce adherence to the defined identity baseline. For this subscription and any others in the new management group, the policies and templates are slightly different. Policies blocking ingress bandwidth have been lifted. They have been replaced by requirements to route traffic through the shared services subscription, like any ingress traffic, to enforce traffic isolation. Since the on-premises operations management tooling can't access this subscription, agents for that tool are no longer required either. All other governance guardrails required by other subscriptions in the management group hierarchy are still enforced, ensuring sufficient guardrails.

The mature creative approach of Contoso's Central IT team provided a solution that didn't compromise

governance or compliance, but still encouraged adoption. This approach of brokering rather than owning cloud-native approaches to centralized IT is the first step toward building a cloud center of excellence (CCoE). Adopting this approach to quickly evolve existing policies will allow for centralized control when required and governance guardrails when more flexibility is acceptable. Balancing these two considerations mitigates the risks associated with centralized IT in the cloud.

## Next steps

- As a central IT team matures its cloud capabilities, the next maturity step is typically looser coupling of cloud operations. The availability of cloud-native operations management tooling and lower operating costs for PaaS-first solutions often lead to business teams (or more specifically, DevOps teams within the business) assuming responsibility for cloud operations.

Learn more about:

- [Building a cloud operations team](#)
- [Cloud operations functions](#)

# Cloud operations functions

11/9/2020 • 2 minutes to read • [Edit Online](#)

An operations team focuses on monitoring, repairing, and the remediation of issues related to traditional IT operations and assets. In the cloud, many of the capital costs and operations activities are transferred to the cloud provider, giving IT operations the opportunity to improve and provide significant additional value.

The skills needed to provide cloud operations functions can be provided by:

- IT operations
- Outsource IT operations vendors
- Cloud service providers
- Cloud-managed service providers
- Application-specific operations teams
- Business application operations teams
- DevOps teams

## IMPORTANT

The individuals or teams accountable for cloud operations are generally responsible for making reactive changes to configuration during remediation. They're also likely to be responsible for proactive configuration changes to minimize operational disruptions. Depending on the organization's cloud operating model, those changes could be delivered via infrastructure-as-code, Azure Pipelines, or direct configuration in the portal. Since operations team will likely have elevated permissions, it is extremely important that those who fill this role are following [identity and access control best practices](#) to minimize unintended access or production changes.

## Preparation

- [Manage resources in Azure](#): Learn how to work through the Azure CLI and web portal to create, manage, and control cloud-based resources.
- [Azure network services](#): Learn Azure networking basics and how to improve resiliency and reduce latency.

Review the following:

- [Business outcomes](#)
- [Financial models](#)
- [Motivations for cloud adoption](#)
- [Business risks](#)
- [Rationalization of the digital estate](#)

## Minimum scope

The duties of the people on the cloud operations team involve delivering maximum workload performance and minimum business interruptions within an agreed-upon operations budget.

- Determine workload criticality, impact of disruptions, or performance degradation.
- Establish business-approved cost and performance commitments.
- Monitor and operate cloud workloads.

# Deliverables

- Maintain asset and workload inventory
- Monitor performance of workloads
- Maintain operational compliance
- Protect workloads and associated assets
- Recover assets if there is performance degradation or business interruption
- Mature functionality of core platforms
- Continuously improve workload performance
- Improve budgetary and design requirements of workloads to fit commitments to the business

## Meeting cadence

The cloud operations team should be involved in release planning and cloud center of excellence planning to provide feedback and prepare for operational requirements.

## Out of scope

Traditional IT operations that focus on maintaining current-state operations for low-level technical assets is out of scope for the cloud operations team. Things like storage, CPU, memory, network equipment, servers, and virtual machine hosts require continuous maintenance, monitoring, repair, and remediation of issues to maintain peak operations. In the cloud, many of these capital costs and operations activities are transferred to the cloud provider.

## Next steps

As adoption and operations scale, it's important to define and automate governance best practices that extend existing IT requirements. Forming a cloud center of excellence is an important step to scaling cloud adoption, cloud operations, and cloud governance efforts.

Learn more about:

- [Cloud center of excellence](#) functions.
- [Organizational antipatterns: Silos and fiefdoms](#).

Learn to align responsibilities across teams by developing a cross-team matrix that identifies responsible, accountable, consulted, and informed (RACI) parties. Download and modify the [RACI template](#).

# Cloud center of excellence (CCoE) functions

11/9/2020 • 9 minutes to read • [Edit Online](#)

Business and technical agility are core objectives of most IT organizations. A cloud center of excellence (CCoE) is a function that creates a balance between speed and stability.

## Function structure

A CCoE model requires collaboration between each of the following:

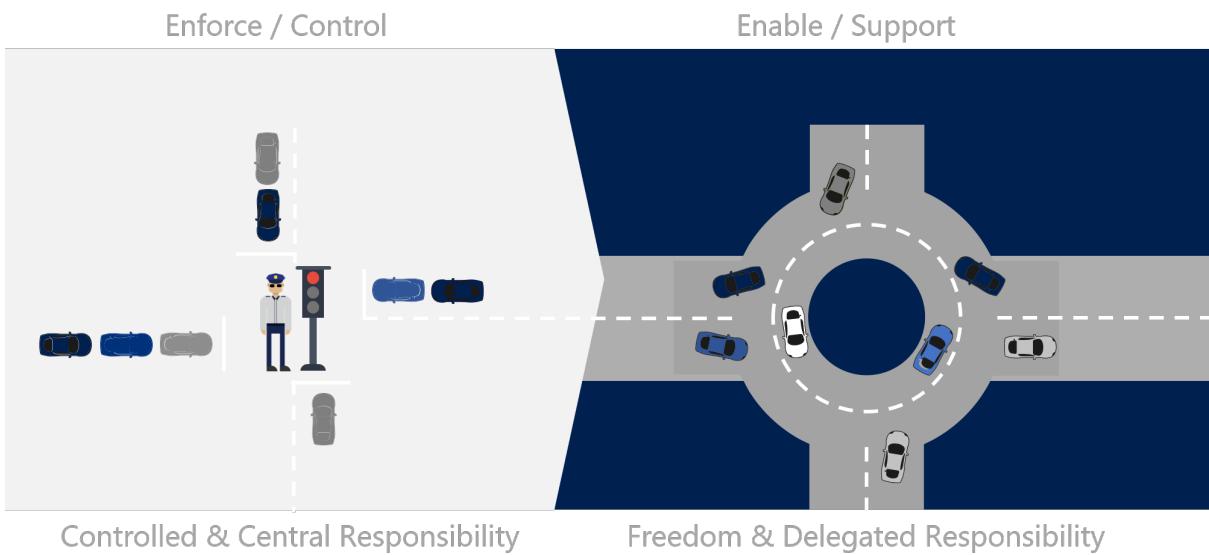
- Cloud adoption (specifically solution architects)
- Cloud strategy (specifically the program and project managers)
- Cloud governance
- Cloud platform
- Cloud automation

## Impact and cultural change

When this function is properly structured and supported, the participants can accelerate innovation and migration efforts while reducing the overall cost of change and increasing business agility. When successfully implemented, this function can produce noticeable reductions in time-to-market. As team practices mature, quality indicators will improve, including reliability, performance efficiency, security, maintainability, and customer satisfaction. These gains in efficiency, agility, and quality are especially vital if the company plans on implementing large-scale cloud migration efforts or has a desire to use the cloud to drive innovations associated with market differentiation.

When successful, a CCoE model will create a significant cultural shift in IT. The fundamental premise of a CCoE approach is that IT serves as a broker, partner, or representative to the business. This model is a paradigm shift away from the traditional view of IT as an operations unit or abstraction layer between the business and IT assets.

The following image provides an analogy for this cultural change. Without a CCoE approach, IT tends to focus on providing control and central responsibility, acting like the stoplights at an intersection. When the CCoE is successful, the focus is on freedom and delegated responsibility, which is more like a roundabout at an intersection.



Neither of the approaches illustrated in the analogy image above is right or wrong, they're just alternative views of responsibility and management. If the desire is to establish a self-service model that allows business units to make their own decisions while adhering to a set of guidelines and established, repeatable controls, then a CCoE model could fit within the technology strategy.

## Key responsibilities

The primary duty of the CCoE team is to accelerate cloud adoption through cloud-native or hybrid solutions.

The objective of the CCoE is to:

- Help build a modern IT organization through agile approaches to capture and implement business requirements.
- Use reusable deployment packages that align with security, compliance, and service management policies.
- Maintain a functional Azure platform in alignment with operational procedures.
- Review and approve the use of cloud-native tools.
- Over time, standardize and automate commonly needed platform components and solutions.

## Meeting cadence

The CCoE is a function staffed by four high demand teams. It is important to allow for organic collaboration and track growth through a common repository/solution catalog. Maximize natural interactions, but minimize meetings. When this function matures, the teams should try to limit dedicated meetings.

Attendance at recurring meetings, like release meetings hosted by the cloud adoption team, will provide data inputs. In parallel, a meeting after each release plan is shared can provide a minimum touch point for this team.

## Solutions and controls

Each member of the CCoE is tasked with understanding the necessary constraints, risks, and protections that led to the current set of IT controls. The collective efforts of the CCoE should turn that understanding into cloud-native (or hybrid) solutions or controls, which enable the desired self-service business outcomes. As solutions are created, they're shared with various teams in the form of controls or automated processes that serve as guardrails for various efforts. Those guardrails help to route the free-flowing activities of various teams, while delegating responsibilities to the participants in various migration or innovation efforts.

Examples of this transition:

SCENARIO	PRE-CCOE SOLUTION	POST-CCOE SOLUTION
Provision a production SQL Server	Network, IT, and data platform teams provision various components over the course of days or even weeks.	The team requiring the server deploys a PaaS instance of Azure SQL Database. Alternatively, a preapproved template could be used to deploy all of the IaaS assets to the cloud in hours.
Provision a development environment	Network, IT, development, and DevOps teams agree to specs and deploy an environment.	The development team defines their own specs and deploys an environment based on allocated budget.
Update security requirements to improve data protection	Networking, IT, and security teams update various networking devices and VMs across multiple environments to add protections.	Cloud governance tools are used to update policies that can be applied immediately to all assets in all cloud environments.

## Negotiations

At the root of any CCoE effort is an ongoing negotiation process. The CCoE team negotiates with existing IT functions to reduce central control. The trade-offs for the business in this negotiation are freedom, agility, and speed. The value of the trade-off for existing IT teams is delivered as new solutions. The new solutions provide the existing IT team with one or more of the following benefits:

- Ability to automate common issues.
- Improvements in consistency (reduction in day-to-day frustrations).
- Opportunity to learn and deploy new technical solutions.
- Reductions in high severity incidents (fewer quick fixes or late-night pager-duty responses).
- Ability to broaden their technical scope, addressing broader topics.
- Participation in higher-level business solutions, addressing the impact of technology.
- Reduction in menial maintenance tasks.
- Increase in technology strategy and automation.

In exchange for these benefits, the existing IT function may be trading the following values, whether real or perceived:

- Sense of control from manual approval processes.
- Sense of stability from change control.
- Sense of job security from completion of necessary yet repetitive tasks.
- Sense of consistency that comes from adherence to existing IT solution vendors.

In healthy cloud-forward companies, this negotiation process is a dynamic conversation between peers and partnering IT teams. The technical details may be complex, but are manageable when IT understands the objective and is supportive of the CCoE efforts. When IT is less than supportive, the following section on enabling CCoE success can help overcome cultural blockers.

## Enable CCoE success

Before proceeding with this model, it is important to validate the company's tolerance for a growth mindset and IT's comfort with releasing central responsibilities. As mentioned above, the purpose of a CCoE is to exchange control for agility and speed.

This type of change takes time, experimentation, and negotiation. There will be bumps and set backs during

this maturation process. But if the team stays diligent and isn't discouraged from experimentation, there is a high probability of success in improving agility, speed, and reliability. One of the biggest factors in success or failure of a CCoE is support from leadership and key stakeholders.

### **Key stakeholders**

IT leadership is the first and most obvious stakeholder. IT managers will play an important part. But the support of the CIO and other executive-level IT leaders is needed during this process.

Less obvious is the need for business stakeholders. Business agility and time-to-market are key motivations for CCoE formation. As such, the key stakeholders should have a vested interest in these areas. Examples of business stakeholders include line-of-business leaders, finance executives, operations executives, and business product owners.

### **Business stakeholder support**

CCoE efforts can be accelerated with support from the business stakeholders. Much of the focus of CCoE efforts is centered around making long-term improvements to business agility and speed. Defining the impact of current operating models and the value of improvements is valuable as a guide and negotiation tool for the CCoE. Documenting the following items is suggested for CCoE support:

- Establish a set of business outcomes and goals that are expected as a result of business agility and speed.
- Clearly define pain points created by current IT processes (such as speed, agility, stability, and cost challenges).
- Clearly define the historical impact of those pain points (such as lost market share, competitor gains in features and functions, poor customer experiences, and budget increases).
- Define business improvement opportunities that are blocked by the current pain points and operating models.
- Establish timelines and metrics related to those opportunities.

These data points are not an attack on IT. Instead, they help CCoE learn from the past and establish a realistic backlog and plan for improvement.

**Ongoing support and engagement:** CCoE teams can demonstrate quick returns in some areas. But the higher-level goals, like business agility and time-to-market, can take much longer. During maturation, there is a high risk of the CCoE becoming discouraged or being pulled off to focus on other IT efforts.

During the first six to nine months of CCoE efforts, we recommend that business stakeholders allocate time to meet monthly with the IT leadership and the CCoE. There is little need for formal ceremony to these meetings. Simply reminding the CCoE members and their leadership of the importance of this program can go along way to driving CCoE success.

Additionally, we recommend that the business stakeholders stay informed of the progress and blockers experienced by the CCoE team. Many of their efforts will seem like technical minutiae. But it is important for business stakeholders to understand the progress of the plan, so they can engage when the team loses steam or becomes distracted by other priorities.

### **IT stakeholder support**

**Support the vision:** A successful CCoE effort requires a great deal of negotiation with existing IT team members. When done well, all of IT contributes to the solution and feels comfortable with the change. When this is not the case, some members of the existing IT team may want to hold on to control mechanisms for various reasons. Support of IT stakeholders will be vital to the success of the CCoE when those situations occur. Encouragement and reinforcement of the overall goals of the CCoE is important to resolve blockers to proper negotiation. On rare occasions, IT stakeholders may even need to step in and break up a deadlock or tied vote to keep the CCoE progressing.

**Maintain focus:** A CCoE can be a significant commitment for any resource-constrained IT team. Removing

strong architects from short-term projects to focus on long-term gains can create difficulty for team members who aren't part of the CCoE. It is important that IT leadership and IT stakeholders stay focused on the goal of the CCoE. The support of IT leaders and IT stakeholders is required to deprioritize the disruptions of day-to-day operations in favor of CCoE duties.

**Create a buffer:** The CCoE team will experiment with new approaches. Some of those approaches won't align well with existing operations or technical constraints. There is a real risk of the CCoE experiencing pressure or recourse from other teams when experiments fail. Encouragement and buffering the team from the consequences of "fast fail" learning opportunities is important. It's equally important to hold the team accountable to a growth mindset, ensuring that they're learning from those experiments and finding better solutions.

## Next steps

A CCoE model requires cloud platform functions and cloud automation functions. The next step is to align cloud platform functions.

Learn more about:

- [Cloud platform functions](#)
- [Cloud automation functions](#)

# Cloud platform functions

11/9/2020 • 2 minutes to read • [Edit Online](#)

The cloud introduces many technical changes as well as opportunities to streamline technical solutions. But general IT principles and business needs stay the same. You still need to protect sensitive business data. If your IT platform depends on a local area network, there's a good chance that you'll need network definitions in the cloud. Users who need to access applications and data will want their current identities to access relevant cloud resources.

While the cloud presents the opportunity to learn new skills, your current architects should be able to directly apply their experiences and subject matter expertise. Cloud platform functions are usually provided by a select group of architects who focus on learning about the cloud platform. These architects then aid others in decision making and the proper application of controls to cloud environments.

The skills needed to provide full platform functionality can be provided by:

- Enterprise architecture
- IT operations
- IT governance
- IT infrastructure
- Networking
- Identity
- Virtualization
- Business continuity and disaster recovery
- Application owners within IT

## Preparation

- [Foundations for cloud architecture](#): A Pluralsight course to help architect the right foundational solutions.
- [Microsoft Azure architecture](#): A Pluralsight course to ground architects in Azure architecture.
- [Azure network services](#): Learn Azure networking basics and how to improve resiliency and reduce latency.

## Review the following:

- [Business outcomes](#)
- [Financial models](#)
- [Motivations for cloud adoption](#)
- [Business risks](#)
- [Rationalization of the digital estate](#)

## Minimum scope

Cloud platform duties center around the creation and support of your cloud platform or landing zones.

The following tasks are typically executed on a regular basis:

- Monitor adoption plans and progress against the [prioritized migration backlog](#).
- Identify and prioritize platform changes that are required to support the migration backlog.

## Meeting cadence:

Cloud platform expertise usually comes from a working team. Expect participants to commit a large portion of their daily schedules to cloud platform work. Contributions aren't limited to meetings and feedback cycles.

## Deliverables

- Build and maintain the cloud platform to support solutions.
- Define and implement the platform architecture.
- Operate and manage the cloud platform.
- Continuously improve the platform.
- Keep up with new innovations in the cloud platform.
- Bring new cloud functionality to support business value creation.
- Suggest self-service solutions.
- Ensure solutions meet existing governance and compliance requirements.
- Create and validate deployment of platform architecture.
- Review release plans for sources of new platform requirements.

## Next steps

As your cloud platform becomes better defined, aligning [cloud automation functions](#) can accelerate adoption. It can also help establish best practices while reducing business and technical risks.

Learn to align responsibilities across teams by developing a cross-team matrix that identifies responsible, accountable, consulted, and informed (RACI) parties. Download and modify the [RACI template](#).

# Cloud automation functions

5/21/2020 • 2 minutes to read • [Edit Online](#)

During cloud adoption efforts, cloud automation functions unlock the potential of DevOps and a cloud-native approach. Expertise in each of these areas can accelerate adoption and innovation.

The skills needed to provide cloud automation functions can be provided by:

- DevOps engineers
- Developers with DevOps and infrastructure expertise
- IT engineers with DevOps and automation expertise

These subject matter experts might be providing functions in other areas such as cloud adoption, cloud governance, or cloud platform. After they demonstrate proficiency at automating complex workloads, you can recruit these experts to deliver automation value.

## Preparation

Before you admit a team member to this group, they should demonstrate three key characteristics:

- Expertise in any cloud platform with a special emphasis on DevOps and automation.
- A growth mindset or openness to changing the way IT operates today.
- A desire to accelerate business change and remove traditional IT roadblocks.

## Minimum scope

The primary duty of cloud automation is to own and advance the solution catalog. The solution catalog is a collection of prebuilt solutions or automation templates. These solutions can rapidly deploy various platforms as required to support needed workloads. These solutions are building blocks that accelerate cloud adoption and reduce the time to market during migration or innovation efforts.

Examples of solutions in the catalog include:

- A script to deploy a containerized application.
- A Resource Manager template to deploy a SQL HA AO cluster.
- Sample code to build a deployment pipeline using Azure DevOps.
- An Azure DevTest Labs instance of the corporate ERP for development purposes.
- Automated deployment of a self-service environment commonly requested by business users.

The solutions in the solution catalog aren't deployment pipelines for a workload. Instead, you might use automation scripts in the catalog to quickly create a deployment pipeline. You might also use a solution in the catalog to quickly provision platform components to support workload tasks like automated deployment, manual deployment, or migration.

## Strategic tasks

- Rationalization of the digital estate:
  - Monitor adoption plans and progress against the prioritized migration backlog.
  - Identify opportunities to accelerate cloud adoption, reduce effort through automation, and improve security, stability, and consistency.
  - Prioritize a backlog of solutions for the solution catalog that delivers the most value given other strategic inputs.

- Review release plans for sources of new automation opportunities.

#### Meeting cadence:

Cloud automation is a working team. Expect participants to commit a large portion of their daily schedules to cloud automation work. Contributions aren't limited to meetings and feedback cycles.

The cloud automation team should align activities with other areas of capability. This alignment might result in meeting fatigue. To ensure cloud automation has sufficient time to manage the solution catalog, you should review meeting cadences to maximize collaboration and minimize disruptions to development activities.

## Deliverables

- Curate or develop solutions based on the prioritized backlog.
- Ensure solutions align to platform requirements.
- Ensure solutions are consistently applied and meet existing governance and compliance requirements.
- Create and validate solutions in the catalog.

## Next steps

As essential cloud functions align, the collective teams can help develop necessary [technical skills](#).

# Cloud data functions

11/9/2020 • 3 minutes to read • [Edit Online](#)

There are multiple audiences involved in an analytics conversation, including the typical seller, database architect, and infrastructure team. In addition, analytics solutions involve influencers, recommenders, and decision-makers from enterprise architecture, data science, business analysts, and executive leadership roles.

Azure Synapse Analytics enables the entire business, from the IT stakeholder to the business analyst, to collaborate on analytics solutions and understand cloud data functions. The following sections discuss these roles in more detail.

## Database administrators and architects

Database administrators and architects are responsible for integrating and routing data sources into a centralized repository. These experts also handle the administration and performance required for the system, and the accessibility and efficiency of query and analytic modeling against that data.

Using Azure Synapse Analytics, database administrators can match their expanding responsibilities for data warehouses and data lakes. They can use familiar languages and tools, such as T-SQL, to run as many workloads as they want. They can assign resources to escalate critical workloads based on intelligent workload importance, workload isolation, and enhanced concurrency capabilities.

## Infrastructure teams

These teams deal with the provisioning and architecture of the underlying compute resources required for large analytics systems. In many cases, they are managing transitions between datacenter-based and cloud-based systems, and current needs for interoperability across both. Disaster recovery, business continuity, and high availability are common concerns.

With Azure Synapse Analytics, IT professionals can protect and manage their organization's data more efficiently. They can enable big data processing with both on-demand and provisioned compute. Through tight integration with Azure Active Directory, the service helps secure access to cloud and hybrid configurations. IT pros can enforce privacy requirements by using data masking, as well as row-level and column-level security.

## Enterprise architects and data engineers

These teams are responsible for putting together complex solutions with components spanning integration across a wide swath of data tools and solutions. These include:

- Structured and unstructured data
- Transformation
- Storage and retrieval
- Analytic modeling
- Message-based middleware
- Data marts
- Geo-redundancy and data consistency
- Dashboarding and reporting

Enterprise architects and data engineers are generally concerned with building effective architectures that work in an integrated manner. Such architectures preserve performance, availability, ease of administration,

flexibility/extensibility, and actionability.

Using Azure Synapse Analytics, data engineers can simplify the steps to wrangle multiple data types from multiple sources, including streaming, transactional, and business data. They can use a code-free visual environment to connect to data sources and ingest, transform, and place data in the data lake.

## Data scientists

Data scientists understand how to build advanced models for huge volumes of critical, yet often disparate data. Their work involves translating the needs of the business into the technology requirements for normalization and transformation of data. They create statistical and other analytical models, and ensure that line-of-business teams can get the analysis they need to run the business.

Using Azure Synapse Analytics, data scientists can build proofs of concept in minutes, and create or adjust end-to-end solutions. They can provision resources as needed, or simply query existing resources on demand across massive amounts of data. They can do their work in a variety of languages, including T-SQL, R, Python, Scala, .NET, and Spark SQL.

## Business analysts

These teams build and use dashboards, reports, and other forms of data visualization to gain rapid insights required for operations. Often, each line-of-business department will have dedicated business analysts who gather and package information and analytics from specialized applications. These specialized apps can be for credit cards, retail banking, commercial banking, treasury, marketing, and other organizations.

Using Azure Synapse Analytics, business analysts can securely access datasets and use Power BI to build dashboards. They can also securely share data within and outside their organization through Azure Data Share.

## Executives

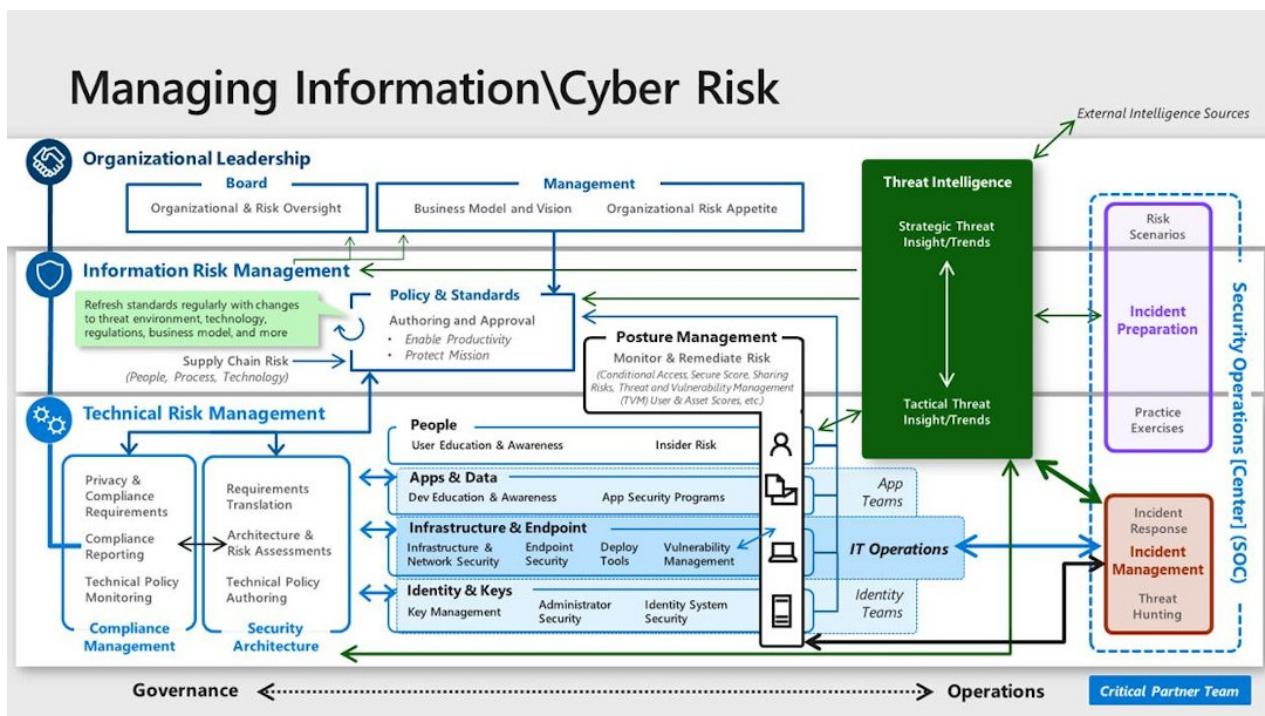
Executives are responsible for charting strategy and ensuring strategic initiatives are implemented effectively across both IT and line-of-business departments. Solutions must be cost-effective, prevent disruption to the business, allow for easy extensibility as requirements change and grow, and deliver results to the business.

# Cloud security functions

11/9/2020 • 2 minutes to read • [Edit Online](#)

This article provides a summary of the organizational functions required to manage information security risk in an enterprise. These organizational functions collectively form the human portion of an overall cybersecurity system. Each function may be performed by one or more people, and each person may perform one or more functions, depending on various factors such as culture, budget, and available resources.

The following diagram and documentation represent an ideal view of the functions of an enterprise security team. The diagram represents an aspirational view for smaller organizations or smaller security teams who might not have significant resources and formal responsibilities defined around all of these functions.



**Security is a team sport:** It's critical that individuals on the security team see each other as part of a whole security team, part of the whole organization, and part of a larger security community defending against the same adversaries. This holistic view enables the team to work well in general. It's especially important as the teams work through any unplanned gaps and overlaps discovered during the evolution of roles and responsibilities.

## Security functions

Each of the following articles provide information about each function. Each article provides a summary of objectives, how the function can evolve because of the threat environment or cloud technology changes, and the relationships and dependencies that are critical to its success.

- [Policy and standards](#)
- [Security operations](#)
- [Security architecture](#)
- [Security compliance management](#)
- [People security](#)
- [Application security and DevSecOps](#)
- [Data security](#)

- Infrastructure and endpoint security
- Identity and key management
- Threat intelligence
- Posture management
- Incident preparation

# Function of cloud security policy and standards

11/9/2020 • 2 minutes to read • [Edit Online](#)

Security policy and standards teams author, approve, and publish security policy and standards to guide security decisions within the organization.

The policies and standards should:

- Reflect the organizations security strategy at a detailed enough way to guide decisions in the organization by various teams
- Enable productivity throughout the organization while reducing risk to the organizations business and mission

**Security policy** should reflect long term sustainable objectives that align to the organizations security strategy and risk tolerance. Policy should always address:

- Regulatory compliance requirements and current compliance status (requirements met, risks accepted, etc.)
- Architectural assessment of current state and what is technically possible to design, implement, and enforce
- Organizational culture and preferences
- Industry best practices
- Accountability of security risk assigned to appropriate business stakeholders who are accountable for other risks and business outcomes.

**Security standards** define the processes and rules to support execution of the security policy.

## Modernization

While policy should remain static, standards should be dynamic and continuously revisited to keep up with pace of change in cloud technology, threat environment, and business competitive landscape.

Because of this high rate of change, you should keep a close eye on how many exceptions are being made as this may indicate a need to adjust standards (or policy).

Security standards should include guidance specific to the adoption of cloud such as:

- Secure use of cloud platforms for hosting workloads
- Secure use of DevOps model and inclusion of cloud applications, APIs, and services in development
- Use of identity perimeter controls to supplement or replace network perimeter controls
- Define your segmentation strategy prior to moving your workloads to IaaS platform
- Tagging and classifying the sensitivity of assets
- Define process for assessing and ensuring your assets are configured and secured properly

## Team composition and key relationships

Cloud security policy and standards are commonly provided by the following types of roles. The organizational policy should inform (and be informed by):

- Security architectures
- Compliance and risk management teams
- Business unit's leadership and representatives
- Information technology
- Audit and legal teams

The policy should be refined based on many inputs/requirements from across the organization, including but not restricted to those depicted in the [security overview diagram](#).

## Next steps

Review the function of a [cloud security operations center](#) (SOC).

# Cloud SOC functions

11/9/2020 • 2 minutes to read • [Edit Online](#)

The main objective of a cloud security operations center (SOC) is to detect, respond to, and recover from active attacks on enterprise assets.

As the SOC matures, security operations should:

- Reactively respond to attacks detected by tools
- Proactively hunt for attacks that slipped past reactive detections

## Modernization

Detecting and responding to threats is currently undergoing significant modernization at all levels.

- **Elevation to business risk management:** SOC is growing into a key component of managing business risk for the organization
- **Metrics and goals:** Tracking SOC effectiveness is evolving from "time to detect" to these key indicators:
  - *Responsiveness* via mean time to acknowledge (MTTA).
  - *Remediation speed* via mean time to remediate (MTTR).
- **Technology evolution:** SOC technology is evolving from exclusive use of static analysis of logs in a SIEM to add the use of specialized tooling and sophisticated analysis techniques. This provides deep insights into assets that provide high quality alerts and investigation experience that complement the breadth view of the SIEM. Both types of tooling are increasingly using AI and machine learning, behavior analytics, and integrated threat intelligence to help spot and prioritize anomalous actions that could be a malicious attacker.
- **Threat hunting:** SOCs are adding hypothesis driven threat hunting to proactively identify advanced attackers and shift noisy alerts out of frontline analyst queues.
- **Incident management:** Discipline is becoming formalized to coordinate nontechnical elements of incidents with legal, communications, and other teams. **Integration of internal context:** To help prioritize SOC activities such as the relative risk scores of user accounts and devices, sensitivity of data and applications, and key security isolation boundaries to closely defend.

For more information, see:

- [Strategy and architecture standards—security operations](#)
- [CISO workshop module 4b: Threat protection strategy](#)
- Cyber Defense Operations Center (CDOC) blog series [part 1](#), [part 2a](#), [part 2b](#), [part 3a](#), [part 3b](#)
- [NIST computer security incident handling guide](#)
- [NIST guide for cybersecurity event recovery](#)

## Team composition and key relationships

The cloud security operations center is commonly made up of the following types of roles.

- IT operations (close regular contact)
- Threat intelligence
- Security architecture
- Insider risk program
- Legal and human resources

- Communications teams
- Risk organization (if present)
- Industry specific associations, communities, and vendors (before incident occurs)

## Next steps

Review the function of [security architecture](#).

# Cloud security architecture functions

11/9/2020 • 2 minutes to read • [Edit Online](#)

Security architecture translates the organization's business and assurance goals into documentation and diagrams to guide technical security decisions.

## Modernization

Security architecture is affected by different factors:

- **Continuous engagement model:** Continuous release of software updates and cloud features make fixed engagement models obsolete. Architects should be engaged with all teams working in technical topic areas to guide decision making along those teams' capability lifecycles.
- **Security from the cloud:** Incorporate security capabilities from the cloud to reduce enablement time and ongoing maintenance costs (hardware, software, time, and effort).
- **Security of the cloud:** Ensure coverage of all cloud assets including software as a service (SaaS) applications, infrastructure as a service (IaaS) VMs, and platform as a service (PaaS) applications and services. This should include discovery and security of both sanctioned and unsanctioned services.
- **Identity integration:** Security architects should ensure tight alignment with identity teams to help organizations meet the dual goals of enabling productivity and providing security assurances.
- **Integration of internal context** in security designs to such as context from posture management and incidents investigated by security operations [center] (SOC). This should include elements like relative risk scores of user accounts and devices, sensitivity of data, and key security isolation boundaries to actively defend.

## Team composition and key relationships

Security architecture is ideally provided by a dedicated individual or dedicated team, but resource constraints may require assigning this function to an individual with other responsibilities.

Security architecture should have a broad portfolio of relationships across the security organization, with key stakeholders in other organizations, and with peers in external organizations. Key internal relationships should include:

- IT/enterprise architects
- Security posture management
- Technology directors
- Key business leaders or their representatives
- Industry peers and others in the security community

Security architects should actively influence [security policy and standards](#).

## Next steps

Review the function of [cloud security compliance management](#).

# Cloud security compliance management functions

11/9/2020 • 2 minutes to read • [Edit Online](#)

The objective of cloud security compliance management is to ensure that the organization is compliant with regulatory requirements (and internal policies) and efficiently tracks and reports status.

## Modernization

Cloud introduces changes to security compliance including:

- **Requirement to validate** the compliance status of the cloud provider with your regulatory requirements. This is a shared responsibility, see adopting the shared responsibility model for how these responsibilities differ for cloud types.
- **Pre-cloud guidance:** While many regulatory requirements have been updated to incorporate the dynamic nature of cloud services, some do not yet include this. Organizations should work with regulatory bodies to get these updated and be prepared to explain these differences during audit exercises.
- **Linking compliance to risk:** Ensure that organizations are tying compliance violations and exceptions to organizational risks to ensure the right level of attention and funding to correct issues.
- **Tracking and reporting enabled by cloud:** This function should actively embrace the software defined nature of cloud as this offers comprehensive logging, configuration data, and analytical insight that make reporting on compliance more efficient than traditional on-premises approaches.
- **Cloud-based compliance tools** are available to facilitate easier reporting of regulatory compliance such as [Microsoft Compliance Manager](#), which can reduce overhead costs of this function.

## Team composition and key relationships

Cloud security compliance management frequently interacts with:

- Security operations
- IT operations
- Organizational compliance/risk management teams
- Audit and legal teams
- Key business leaders or their representatives

## Next steps

Review the function of [people security](#).

# People security functions in the cloud

11/9/2020 • 2 minutes to read • [Edit Online](#)

People security protects the organization from risk of inadvertent human mistakes and malicious insider actions.

## Modernization

Modernization of this function includes:

- **Increase positive engagement** with users using gamification and positive reinforcement / education rather than relying solely on negative reinforcement approaches like traditional "phish and punish" solutions.
- **High quality human engagement:** Security awareness communications and training should be high quality productions that drive empathy and emotional engagement to connect with the human side of employees and the organizations mission.
- **Realistic expectations:** Accept that users will sometimes open phishing emails, and instead focus success metrics on reducing the rate versus expecting to stop 100 percent of opening.
- **Organizational culture change:** Organizational leadership must drive an intentional culture change to make security a priority for each member of the organization.
- **Increased insider risk focus** to help organizations protect valuable trade secrets and other data with highly profitable illicit use cases (such as customer locations or communication records).
- **Improved insider risk detection** which takes advantage of cloud capabilities for activity logging, behavior analytics, and machine learning (machine learning).

## Team composition and key relationships

People security commonly partners with the following types of roles:

- Audit and legal teams
- Human resources
- Privacy team
- Data security
- Communications teams, for user awareness
- Security operations, for insider risk
- Physical security, for insider risk

## Next steps

Review the function of [application security and DevSecOps](#).

# Application security and DevSecOps functions

11/9/2020 • 2 minutes to read • [Edit Online](#)

The objective of application security and DevSecOps is to integrate security assurances into development processes and custom line of business (LOB) applications.

## Modernization

Application development is rapidly being reshaped in multiple aspects simultaneously including the DevOps team model, DevOps rapid release cadence, and the technical composition of applications via cloud services and APIs. See how the cloud is changing security relationships and responsibilities to understand these changes.

This modernization of antiquated development models presents both opportunity and a requirement to modernize security of applications and development processes. The fusion of security into DevOps processes is often referred to as DevSecOps and drives changes including:

- **Security is integrated, not outside approval:** The rapid pace of change in application development makes classic arms-length "scan and report" approaches obsolete. These legacy approaches can't keep up with releases without grinding development to a halt and creating time-to-market delays, developer underutilization, and growth of issue backlog.
  - **Shift left** to engage security earlier in application development processes as fixing issues earlier is cheaper, faster, and more effective. If you wait until after the cake is baked, it is harder to change the shape.
  - **Native integration:** Security practices must be integrated seamlessly to avoid unhealthy friction in development workflows and continuous integration/continuous deployment (CI/CD) processes. For more information about the GitHub approach, see [Securing software, together](#).
  - **High-quality security:** Security must provide high-quality findings and guidance that enable developers to fix issues fast and don't waste developer time with false positives.
  - **Converged culture:** Security, development, and operations roles should contribute key elements into a shared culture, shared values, and shared goals and accountabilities.
- **Agile security:** Shift security from a "must be perfect to ship" approach to an agile approach that starts with minimum viable security for applications (and for the processes to develop them) that is continuously improved incrementally.
- **Embrace cloud-native infrastructure and security features** to streamline development processes while integrating security.
- **Supply chain risk management:** Take a zero-trust approach to open-source software (OSS) and third-party components that validate their integrity and ensure that bug fixes and updates are applied to these components.
- **Continuous learning:** The rapid release pace of developer services, sometimes called platform as a service (PaaS) services, and changing composition of applications means that dev, ops, and security team members will be constantly learning new technology.
- **Programmatic approach** to application security to ensure continuous improvement of the agile approach happens.

For additional context, see [Microsoft secure development lifecycle](#).

## Team composition and key relationships

Application security and DevSecOps functions are ideally performed by security aware developers and operations

teams (with the support of security subject matter experts).

This function commonly interacts with other functions and experts including:

- Security architecture and operations
- Infrastructure security
- Communications (training and tooling)
- People security
- Identity and keys
- Compliance/risk management teams
- Key business leaders or their representatives

## Next steps

Review the function of [data security](#).

# Function of cloud data security

11/9/2020 • 2 minutes to read • [Edit Online](#)

The main objective for a data security team is to provide security protections and detective controls for sensitive enterprise data in any format in any location.

## Modernization

Data security strategies are being shaped primarily by:

- **Data sprawl:** Sensitive data is being generated and stored on a nearly limitless variety of devices and cloud services where people creatively collaborate.
- **New model:** The cloud enables new models of "phone home for key" to supplement and replace classic data loss protection (DLP) models that "catch it on the way out the door"
- **Regulations** like general data protection regulation (GDPR) are requiring organizations to closely track private data and how applications are using it.

## Team composition and key relationships

Data security commonly interacts with following roles in the organization:

- Key business leaders or their representatives
- Records management teams
- Policy and standards teams
- Privacy teams
- IT architecture and operations
- Security architecture and operations
- Legal teams
- Insider risk team
- Compliance/risk management teams

## Next steps

Review the function of [cloud infrastructure and endpoint security](#).

# Function of cloud infrastructure and endpoint security

11/9/2020 • 2 minutes to read • [Edit Online](#)

A cloud security team working on infrastructure and endpoint security provides security protections, detective, and response controls for infrastructure and network components used by enterprise applications and users.

## Modernization

Software defined datacenters and other cloud technologies are helping solve longstanding challenges with infrastructure and endpoint security including:

- **Inventory and configuration error discovery** are much more reliable for cloud hosted assets as they're all immediately visible (vs. A physical datacenter).
- **Vulnerability management** evolving into a critical part of overall security posture management.
- **Addition of container technologies** to be managed and secured by infrastructure and network teams as the organization adopts this technology broadly. See [container security in Security Center](#) for an example.
- **Security agent consolidation** and tool simplification to reduce the maintenance and performance overhead of security agents and tools.
- **Allow-listing of applications** and internal network filtering is becoming much easier to configure and deploy for cloud hosted servers (using machine learning generated rule sets). See [adaptive application controls](#) and [adaptive network hardening](#) for Azure examples.
- **Automated templates** for configuring infrastructure and security are much easier with software defined datacenters in the cloud. Azure example is [Azure Blueprints](#)
- **Just in time (JIT) and just enough access (JEA)** enable practical application of least privilege principles to privileged access for servers and endpoints.
- **User experience** becomes critical as users increasingly can choose or purchase their endpoint devices.
- **Unified endpoint management** allows managing security posture of all endpoint devices including mobile and traditional PCs as well as providing critical device integrity signals for zero trust access control solutions.
- **Network security architectures** and controls are partially diminished with the shift to cloud application architectures, but they remain a fundamental security measure. For more information, see [Network security and containment](#).

## Team composition and key relationships

Cloud infrastructure and endpoint security commonly interacts with the following roles:

- IT architecture and operations
- Security architecture
- Security operations center (SOC)
- Compliance team
- Audit team

## Next steps

Review the function of [threat intelligence](#).

# Function of identity and key management in the cloud

11/9/2020 • 2 minutes to read • [Edit Online](#)

The main objective of a security team working on identity management is to provide authentication and authorization of humans, services, devices, and applications. Key and certification management provides secure distribution and access to key material for cryptographic operations (which often support similar outcomes as identity management).

## Modernization

Data identity and key management modernization is being shaped by:

- Identity and key/certification management disciplines are coming closer together as they both provide assurances for authentication and authorization to enable secure communications.
- Identity controls are emerging as a primary security perimeter for cloud applications
- Key-based authentication for cloud services is being replaced with identity management because of the difficulty of storing and securely providing access to those keys.
- Critical importance of carrying positive lessons learned from on-premises identity architectures such as single identity, single sign-on (SSO), and native application integration.
- Critical importance of avoiding common mistakes of on-premises architectures that often overcomplicated them, making support difficult and attacks easier. These include:
  - Sprawling groups and organizational units (OUs).
  - Sprawling set of third-party directories and identity management systems.
  - Lack of clear standardization and ownership of application identity strategy.
- Credential theft attacks remain a high impact and high likelihood threat to mitigate.
- Service accounts and application accounts remaining a top challenge, but becoming easier to solve. Identity teams should actively embrace the cloud capabilities that are beginning to solve this like [Azure AD managed identities](#).

## Team composition and key relationships

Identity and key management teams need to build strong relationships with the following roles:

- IT architecture and operations
- Security architecture and operations
- Development teams
- Data security teams
- Privacy teams
- Legal teams
- Compliance/risk management teams

## Next steps

Review the function of [infrastructure and endpoint security](#)

# Function of cloud threat intelligence

11/9/2020 • 2 minutes to read • [Edit Online](#)

Security threat intelligence provides context and actionable insights on active attacks and potential threats to enable decision making by security teams, technical teams, and organizational leaders.

## Modernization

Threat intelligence teams are emerging and evolving to meet the needs of the security operations center (SOC) and others managing security risk for the organization.

These teams should focus on a strategy that includes:

- **Strategic threat intelligence** tailored to executive audiences increases awareness of cybersecurity risk, funding requirements, and supports sound risk decision making by organizational leadership.
- **Incremental program growth** to provide quick wins with direct incident support and evolving into a threat intelligence platform to track and inform stakeholders.
- **Tactical and operational threat intelligence** to guide decision making during incident investigation and threat detections.

## Team composition and key relationships

Cloud threat intelligence is commonly provided by the following types of roles.

- Security posture management
- Organizational executive leadership
- Key business leaders or their representatives
- Security architecture and operations
- IT architecture and operations
- Risk management teams

## Next steps

Review the function of cloud security posture management.

# Function of cloud security posture management

11/9/2020 • 2 minutes to read • [Edit Online](#)

The main objective for a cloud security team working on posture management is to continuously report on and improve the security posture of the organization by focusing on disrupting a potential attacker's return on investment (ROI).

## Modernization

Posture management is a set of new functions that realize many previously imagined or attempted ideas that were difficult, impossible, or extremely manual before the advent of the cloud. Some of elements of posture management can be traced to zero trust, deperimeterization, continuous monitoring, and manual scoring of risk by expert consultancies.

Posture management introduces a structured approach to this, using the following:

- **Zero trust-based access control:** That considers active threat level during access control decisions.
- **Real time risk scoring:** To provide visibility into top risks.
- **Threat and vulnerability management (TVM)** to establish a holistic view of the organizations attack surface and risk and integrate it into operations and engineering decision making.
- **Discover sharing risks:** To understand the data exposure of enterprise intellectual property on both sanctioned and unsanctioned cloud services.
- **Cloud security posture management** to take advantage of cloud instrumentation to monitor and prioritize security improvements.
- **Technical policy:** Apply guardrails to audit and enforce the organizations standards and policies to technical systems. See Azure Policy and [Azure Blueprints](#).
- **Threat modelling** systems and architectures, as well as specific applications.

**Emerging discipline:** Security posture management will disrupt many norms of the security organization in a healthy way with these new capabilities and may shift responsibilities among roles or create new roles.

## Team composition and key relationships

Security posture management is an evolving function, so it may be a dedicated team or may it be provided by other teams.

Security posture management should work closely with the following teams:

- Threat intelligence team
- Information technology
- Compliance and risk management teams
- Business leaders and SMEs
- Security architecture and operations
- Audit team

## Next steps

Review the function of cloud security [incident preparation](#).

# Function of cloud security incident preparation

11/9/2020 • 2 minutes to read • [Edit Online](#)

The primary objective for an incident preparation team is to build process maturity and muscle memory for responding to major incidents throughout the organization. This includes helping prepare security, executive leadership and many outside of security.

## Modernization

Practice exercises have become powerful tools to ensure stakeholders are informed and familiar with their role in a major security incident. Participants of these exercises should include:

- **Executive leadership and board of directors** to make strategic risk decisions and provide oversight.
- **Communications and public relations** to ensure internal users, customers, and other external stakeholders are informed of relevant and appropriate information.
- **Internal stakeholders** to provide legal counsel and other business advice
- **Incident management** to coordinate activities and communications.
- **Technical team members** to investigate and remediate incident.
- **Business continuity integration** with organizational functions that own crisis management, disaster recovery, and business continuity plans.

Microsoft has published lessons learned and recommendations in the [incident response reference guide \(IRRG\)](#).

## Team composition and key relationships

Critical partners for security incident preparation are:

- Security operations center (SOC).
- External counsel as needed.
- Media and communication training.
- External partners and government agencies, if applicable.

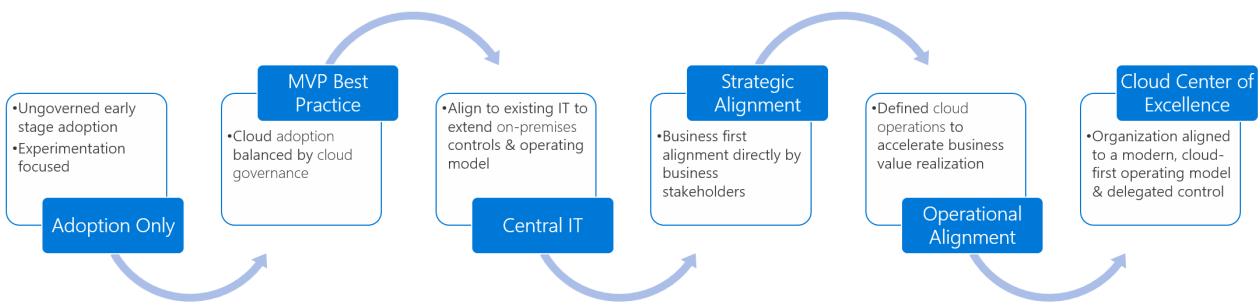
# Mature team structures

11/9/2020 • 5 minutes to read • [Edit Online](#)

Every cloud function is provided by someone during every cloud adoption effort. These assignments and team structures can develop organically, or they can be intentionally designed to match a defined team structure.

As adoption needs grow, so does the need for balance and structure. Watch this video to get an overview of common team structures at various stages of organizational maturity.

The following graphic and list outline those structures based on typical maturation stages. Use these examples to find the organizational structure that best aligns with your operational needs.



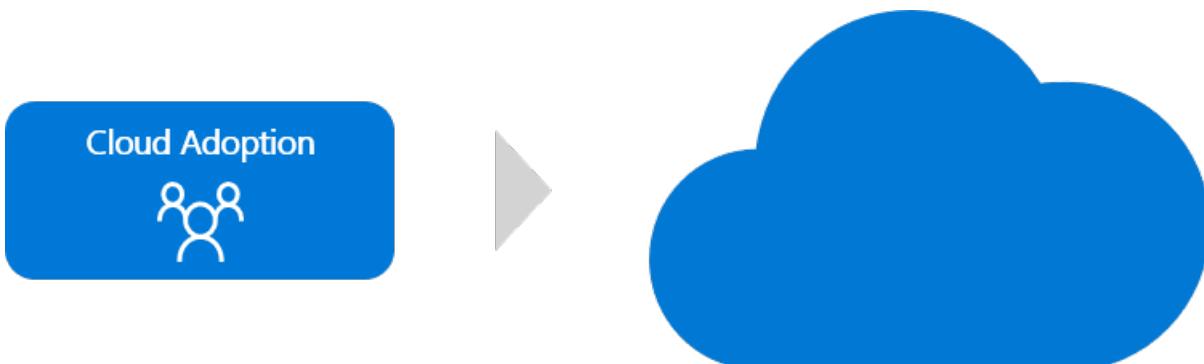
Organizational structures tend to move through the common maturity model that's outlined here:

1. [Cloud adoption team only](#)
2. [MVP best practice](#)
3. [Central IT team](#)
4. [Strategic alignment](#)
5. [Operational alignment](#)
6. [Cloud center of excellence \(CCoE\)](#)

Most companies start with little more than a *cloud adoption team*. But we recommend that you establish an organizational structure that more closely resembles the [MVP best practice](#) structure.

## Cloud adoption team only

The nucleus of all cloud adoption efforts is the cloud adoption team. This team drives the technical changes that enable adoption. Depending on the objectives of the adoption effort, this team might include a diverse range of team members who handle a broad set of technical and business tasks.



For small-scale or early-stage adoption efforts, this team might be as small as one person. In larger-scale or late-

stage efforts, it's common to have several cloud adoption teams, each with around six engineers. Regardless of size or tasks, the consistent aspect of any cloud adoption team is that it provides the means to onboarding solutions into the cloud. For some organizations, this might be a sufficient organizational structure. The [cloud adoption team](#) article provides more insight into the structure, composition, and function of the cloud adoption team.

#### WARNING

Operating with **only** a cloud adoption team (or multiple cloud adoption teams) is considered an antipattern and should be avoided. At a minimum, consider the [MVP best practice](#).

## Best practice: Minimum viable product (MVP)



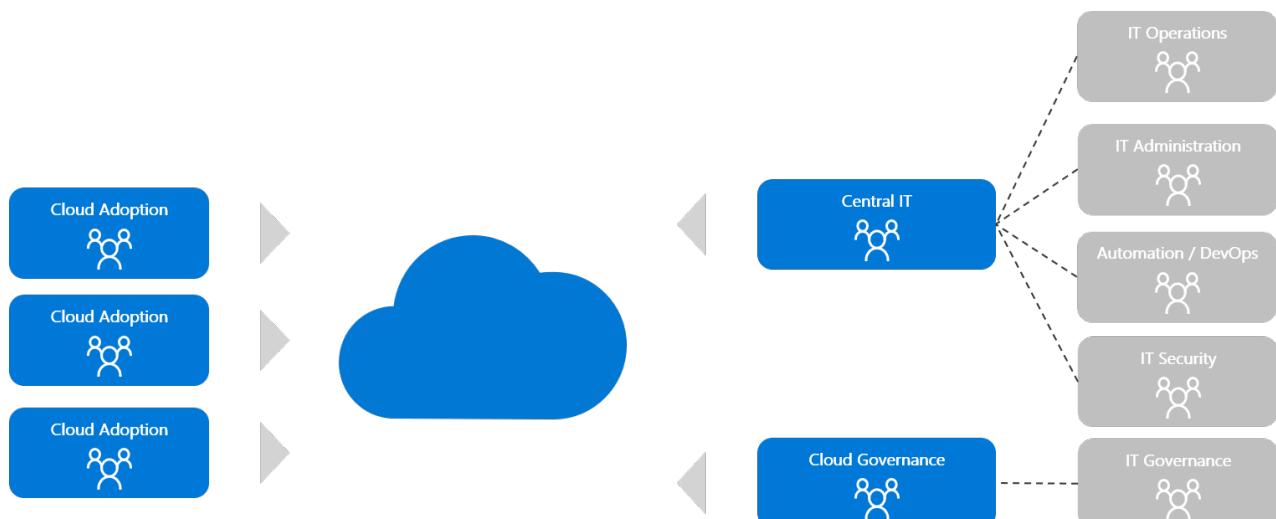
We recommend that you have two teams to create balance across cloud adoption efforts. These two teams are responsible for various functions throughout the adoption effort.

- **Cloud adoption team:** This team is accountable for technical solutions, business alignment, project management, and operations for solutions that are adopted.
- **Cloud governance team:** To balance the cloud adoption team, a cloud governance team is dedicated to ensuring excellence in the solutions that are adopted. The cloud governance team is accountable for platform maturity, platform operations, governance, and automation.

This proven approach is considered an MVP because it might not be sustainable. Each team is wearing many hats, as outlined in the [responsible, accountable, consulted, informed \(RACI\) charts](#).

The following sections describe a fully staffed, proven organizational structure along with approaches to aligning the appropriate structure to your organization.

## Central IT team



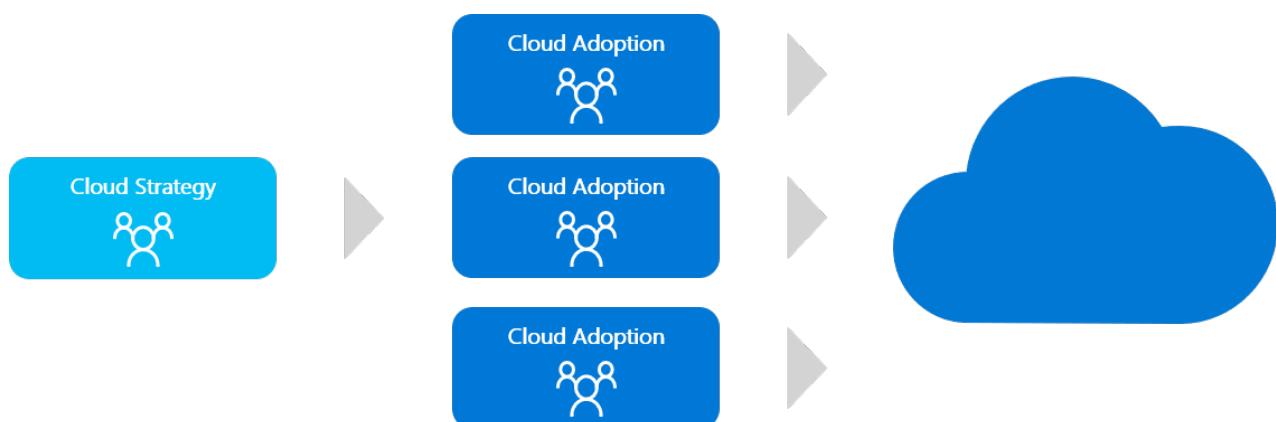
As adoption scales, the cloud governance team might struggle to keep pace with the flow of innovation from multiple cloud adoption teams. This is especially true in environments that have heavy compliance, operations, or security requirements. At this stage, it is common for companies to shift cloud responsibilities to an existing central IT team. If that team can reassess tools, processes, and people to better support cloud adoption at scale, then

including the central IT team can add significant value. Bringing in subject matter experts from operations, automation, security, and administration to modernize the central IT team can drive effective operational innovations.

Unfortunately, the central IT team phase can be one of the riskiest phases of organizational maturity. The central IT team must come to the table with a strong growth mindset. If the team views the cloud as an opportunity to grow and adapt, then it can provide great value throughout the process. But if the central IT team views cloud adoption primarily as a threat to their existing model, then the central IT team becomes an obstacle to the cloud adoption teams and the business objectives they support. Some central IT teams have spent months or even years attempting to force the cloud into alignment with on-premises approaches, with only negative results. The cloud doesn't require that everything change within the central IT team, but it does require significant change. If resistance to change is prevalent within the central IT team, this phase of maturity can quickly become a cultural antipattern.

Cloud adoption plans heavily focused on platform as a service (PaaS), DevOps, or other solutions that require less operations support are less likely to see value during this phase of maturity. On the contrary, these types of solutions are the most likely to be hindered or blocked by attempts to centralize IT. A higher level of maturity, like a [cloud center of excellence \(CCoE\)](#), is more likely to yield positive results for those types of transformational efforts. To understand the differences between centralized IT in the cloud and a CCoE, see [Cloud center of excellence](#).

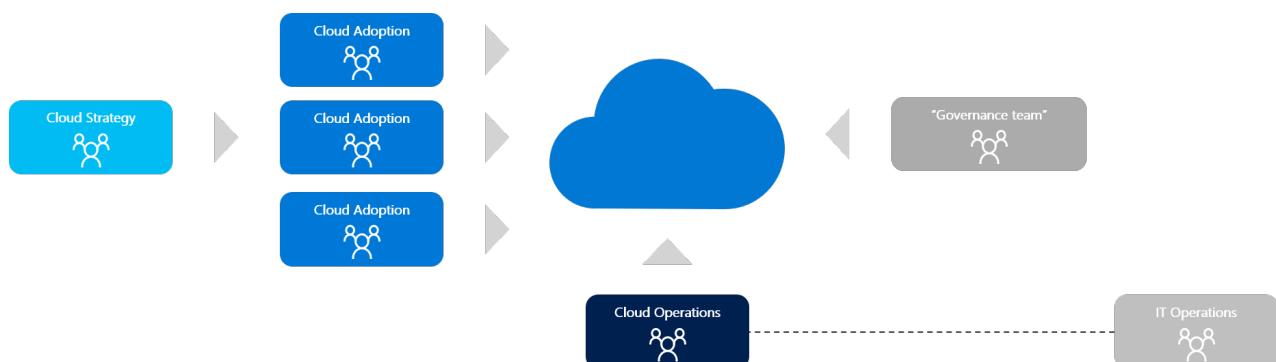
## Strategic alignment



As the investment in cloud adoption grows and business values are realized, business stakeholders often become more engaged. A defined cloud strategy team, as the following image illustrates, aligns those business stakeholders to maximize the value realized by cloud adoption investments.

When maturity happens organically, as a result of IT-led cloud adoption efforts, strategic alignment is usually preceded by a governance or central IT team. When cloud adoption efforts are lead by the business, the focus on operating model and organization tends to happen earlier. Whenever possible, business outcomes and the cloud strategy team should both be defined early in the process.

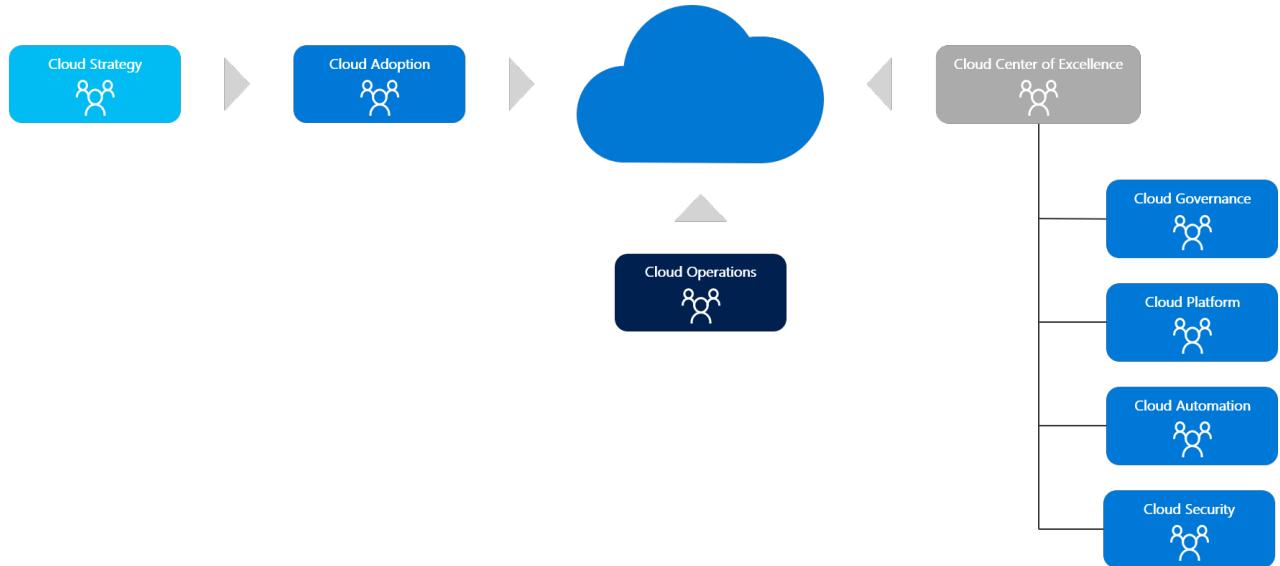
## Operational alignment



Realizing business value from cloud adoption efforts requires stable operations. Operations in the cloud might require new tools, processes, or skills. When stable IT operations are required to achieve business outcomes, it's important to add a defined cloud operations team, as shown here.

Cloud operations can be delivered by the existing IT operations roles. But it's not uncommon for cloud operations to be delegated to other parties outside of IT operations. Managed service providers, DevOps teams, and business unit IT often assume the responsibilities associated with cloud operations, with support and guardrails provided by IT operations. This is increasingly common for cloud adoption efforts that focus heavily on DevOps or PaaS deployments.

## Cloud center of excellence



At the highest state of maturity, a cloud center of excellence aligns teams around a modern cloud-first operating model. This approach provides centralized IT functions like governance, security, platform, and automation.

The primary difference between this structure and the central IT team structure above is a strong focus on self-service and democratization. The teams in this structure organize with the intent of delegating control as much as possible. Aligning governance and compliance practices to cloud-native solutions creates guardrails and protection mechanisms. Unlike the central IT team model, the cloud-native approach maximizes innovation and minimizes operational overhead. For this model to be adopted, mutual agreement to modernize IT processes will be required from business and IT leadership. This model is unlikely to occur organically and often requires executive support.

## Next steps

After aligning to a certain stage of organizational structure maturity, you can use [RACI charts](#) to align accountability and responsibility across each team.

[Align the appropriate RACI chart](#)

# Align responsibilities across teams

11/9/2020 • 3 minutes to read • [Edit Online](#)

Learn to align responsibilities across teams by developing a cross-team matrix that identifies *responsible, accountable, consulted, and informed (RACI)* parties. This article provides an example RACI matrix for the organizational structures described in [Establish team structures](#):

- Cloud adoption team only
  - MVP best practice
  - Central IT team
  - Strategic alignment
  - Operational alignment
  - Cloud center of excellence (CCoE)

To track organizational structure decisions over time, download and modify the RACI template.

The examples in this article specify these RACI constructs:

- The one team that is *accountable* for a function.
  - The teams that are *responsible* for the outcomes.
  - The teams that should be *consulted* during planning.
  - The teams that should be *informed* when work is completed.

The last row of each table (except the first) contains a link to the most-aligned cloud capability for additional information.

## Cloud adoption team only

## Best practice: Minimum viable product (MVP)

TEAM	SOLUTION DELIVERY	BUSINESS ALIGNMENT	CHANGE MANAGEMENT	SOLUTION OPERATIONS	GOVERNANCE	PLATFORM MATURITY	PLATFORM OPERATIONS	PLATFORM AUTOMATION
Aligned cloud capability	Cloud adoption	Cloud strategy	Cloud strategy	Cloud operations	CCoE and cloud governance	CCoE - cloud platform	CCoE and cloud platform	CCoE and cloud automation

## Central IT team

TEAM	SOLUTION DELIVERY	BUSINESS ALIGNMENT	CHANGE MANAGEMENT	SOLUTION OPERATIONS	GOVERNANCE	PLATFORM MATURITY	PLATFORM OPERATIONS	PLATFORM AUTOMATION
Cloud adoption team	Accountable	Accountable	Responsible	Responsible	Informed	Informed	Informed	Informed
Cloud governance team	Consulted	Informed	Informed	Informed	Accountable	Consulted	Responsible	Informed
Central IT team	Consulted	Informed	Accountable	Accountable	Responsible	Accountable	Accountable	Accountable
Aligned cloud capability	Cloud adoption	Cloud strategy	Cloud strategy	Cloud operations	Cloud governance	Central IT team	Central IT team	Central IT team

## Strategic alignment

TEAM	SOLUTION DELIVERY	BUSINESS ALIGNMENT	CHANGE MANAGEMENT	SOLUTION OPERATIONS	GOVERNANCE	PLATFORM MATURITY	PLATFORM OPERATIONS	PLATFORM AUTOMATION
Cloud strategy team	Consulted	Accountable	Accountable	Consulted	Consulted	Informed	Informed	Informed
Cloud adoption team	Accountable	Consulted	Responsible	Accountable	Informed	Informed	Informed	Informed
CCoE model RACI	Consulted	Informed	Informed	Informed	Accountable	Accountable	Accountable	Accountable
Aligned cloud capability	Cloud adoption	Cloud strategy	Cloud strategy	Cloud operations	CCoE and cloud governance	CCoE and cloud platform	CCoE and cloud platform	CCoE and cloud automation

# Operational alignment

TEAM	SOLUTION DELIVERY	BUSINESS ALIGNMENT	CHANGE MANAGEMENT	SOLUTION OPERATIONS	GOVERNANCE	PLATFORM MATURITY	PLATFORM OPERATIONS	PLATFORM AUTOMATION
Cloud strategy team	Consulted	Accountable	Accountable	Consulted	Consulted	Informed	Informed	Informed
Cloud adoption team	Accountable	Consulted	Responsible	Consulted	Informed	Informed	Informed	Informed
Cloud operations team	Consulted	Consulted	Responsible	Accountable	Consulted	Informed	Accountable	Consulted
CCoE model RACI	Consulted	Informed	Informed	Informed	Accountable	Accountable	Responsible	Accountable
Aligned cloud capability	Cloud adoption	Cloud strategy	Cloud strategy	Cloud operations	CCoE and cloud governance	CCoE and cloud platform	CCoE and cloud platform	CCoE and cloud automation

# Cloud center of excellence (CCoE)

TEAM	SOLUTION DELIVERY	BUSINESS ALIGNMENT	CHANGE MANAGEMENT	SOLUTION OPERATIONS	GOVERNANCE	PLATFORM MATURITY	PLATFORM OPERATIONS	PLATFORM AUTOMATION
Cloud strategy team	Consulted	Accountable	Accountable	Consulted	Consulted	Informed	Informed	Informed
Cloud adoption team	Accountable	Consulted	Responsible	Consulted	Informed	Informed	Informed	Informed
Cloud operations team	Consulted	Consulted	Responsible	Accountable	Consulted	Informed	Accountable	Consulted
Cloud governance team	Consulted	Informed	Informed	Consulted	Accountable	Consulted	Responsible	Informed
Cloud platform team	Consulted	Informed	Informed	Consulted	Consulted	Accountable	Responsible	Responsible

TEAM	SOLUTION DELIVERY	BUSINESS ALIGNMENT	CHANGE MANAGEMENT	SOLUTION OPERATIONS	GOVERNANCE	PLATFORM MATURITY	PLATFORM OPERATIONS	PLATFORM AUTOMATION
Cloud automation team	Consulted	Informed	Informed	Informed	Consulted	Responsible	Responsible	Accountable
Aligned cloud capability	Cloud adoption	Cloud strategy	Cloud strategy	Cloud operations	CCoE and cloud governance	CCoE and cloud platform	CCoE and cloud platform	CCoE and cloud automation

## Next steps

To track decisions about organization structure over time, download and modify the RACI template. Copy and modify the most closely aligned sample from the RACI matrices in this article.

[Download the RACI template](#)

# Build technical skills

11/9/2020 • 3 minutes to read • [Edit Online](#)

Organizational and environmental (technical) readiness can require new skills for technical and nontechnical contributors. The following information can help your organization build the necessary skills.

## Organizational readiness learning paths

Depending on the motivations and business outcomes that are associated with a cloud-adoption effort, leaders may need to establish new organizational structures or virtual teams to facilitate various functions. The following articles can help your organization develop the necessary skills to structure those teams to meet the desired outcomes:

- [Align your organization](#): Discover approaches to establishing the proper organizational structures.
- [Organization alignment exercises](#): Get an overview of alignment and team structures to help meet specific goals.
- [Establish teams](#): Learn how to establish teams within your organization that are responsible for delivering cloud functionality.
- [Break down silos and fiefdoms](#): Learn about two common organizational antipatterns and ways to guide the teams to productive collaboration.

## Environmental (technical) readiness learning paths

During the Ready phase, technical staff have to create a migration landing zone to host, operate, and govern workloads that they migrate to the cloud. Use the following paths to accelerate development of the necessary skills:

- [Create an Azure account](#): The first step to using Azure is to create an account. Your account holds the Azure services that you provision and handles your personal settings, like identity, billing, and preferences.
- [Azure portal](#): Tour the Azure portal features and services, and customize the portal.
- [Introduction to Azure](#): Get started with Azure. Create and configure your first virtual machine in the cloud.
- [Introduction to security in Azure](#): Learn the basic concepts to protect your infrastructure and data in the cloud. Understand what responsibilities are yours and what Azure handles.
- [Manage resources in Azure](#): Learn how to work through the Azure CLI and web portal to create, manage, and control cloud-based resources.
- [Create a VM](#): Use the Azure portal to create a virtual machine.
- [Azure network services](#): Learn Azure networking basics and how to improve resiliency and reduce latency.
- [Azure compute options](#): Review the Azure compute services.
- [Secure resources with RBAC](#): Use role-based access control (RBAC) to secure resources.
- [Azure Storage options](#): Learn about the benefits of Azure data storage.

During the Ready phase, architects have to design solutions that span all Azure environments. The following resources can prepare them for these tasks:

- [Foundations for cloud architecture](#): A Pluralsight course to help architect the right foundational solutions.
- [Microsoft Azure architecture](#): A Pluralsight course to ground architects in Azure architecture.
- [Designing migrations for Microsoft Azure](#): A Pluralsight course to help architects design a migration solution.

# Deeper skills exploration

The following information describes resources for additional learning.

## Typical mappings of cloud IT roles

Microsoft and its partners offer options to help all audiences develop their skills for using Azure services.

- [Microsoft IT Pro Career Center](#): A free online resource to help map your cloud career path. Learn from industry experts about your cloud role and the skills you need. Follow a learning curriculum at your own pace to build the skills that you need to stay relevant.

We recommend that you turn your knowledge of Azure into official recognition with [Microsoft Azure certification training and exams](#).

## Microsoft Learn

Microsoft Learn is a new approach to learning. Readiness for the new responsibilities that come with cloud adoption doesn't come easily. Microsoft Learn provides a rewarding approach to hands-on learning that helps you achieve your goals faster. Earn points, reach new levels, and achieve more.

The following are a few examples of role-specific learning paths on Microsoft Learn:

- [Business users](#) may experience a steep learning curve when they help plan, test, and adopt cloud-based technology. Microsoft Learn modules focus on adopting cloud models and tools for better managing business through cloud-based services.
- [Solution architects](#) can access hundreds of modules and learning paths. The available topics range from core infrastructure services to advanced data transformation.
- [Administrators](#) have access to modules that focus on Azure fundamentals, configuring containers, and even advanced administration in the cloud.
- [Developers](#) can use Microsoft Learn resources to help during architecture, governance, modernization activities.

## Learn more

For additional learning paths, browse the [Microsoft Learn catalog](#). Use the roles filter to align learning paths with your role.

# Build a cost-conscious organization

5/22/2020 • 6 minutes to read • [Edit Online](#)

As outlined in [Motivations: why are we moving to the cloud?](#), there are many sound reasons for a company to adopt the cloud. When cost reduction is a primary driver, it's important to create a cost-conscious organization.

Ensuring cost consciousness is not a one-time activity. Like other cloud-adoption topics, it's iterative. The following diagram outlines this process to focus on three interdependent activities: *visibility*, *accountability*, and *optimization*. These processes play out at macro and micro levels, which we describe in detail in this article.



Figure 1: Outline of the cost-conscious organization.

## General cost-conscious processes

- **Visibility:** For an organization to be conscious of costs, it needs visibility into those costs. Visibility in a cost-conscious organization requires consistent reporting for the teams adopting the cloud, finance teams who manage budgets, and management teams who are responsible for the costs. This visibility is accomplished by establishing:
  - The right reporting scope.
  - Proper resource organization (management groups, resource groups, subscriptions).
  - Clear tagging strategies.
  - Proper access controls (RBAC).
- **Accountability:** Accountability is as important as visibility. Accountability starts with clear budgets for adoption efforts. Budgets should be well established, clearly communicated, and based on realistic expectations. Accountability requires an iterative process and a growth mindset to drive the right level of accountability.
- **Optimization:** Optimization is the action that creates cost reductions. During optimization, resource allocations are modified to reduce the cost of supporting various workloads. This process requires iteration and experimentation. Each reduction in cost reduces performance. Finding the right balance between cost control and end-user performance expectations demands input from multiple parties.

The following sections describe the roles that various teams play in developing a cost-conscious organization.

## Cloud strategy team

Building cost consciousness into cloud-adoption efforts starts at the leadership level. To be effective in the long term, the [cloud strategy team](#) should include a member of the finance team. If your financial structure holds business managers accountable for solution costs, they should be invited to join the team as well. In addition to the core activities that are typically assigned to the cloud strategy team, all members of the cloud strategy team should also be responsible for:

- **Visibility:** The cloud strategy team and [cloud governance team](#) need to know the actual costs of the cloud-adoption efforts. Given the executive-level view of this team, they should have access to multiple cost scopes to analyze spending decisions. Typically, an executive needs visibility into the total costs across all cloud "spend." But as active members of the cloud strategy team, they should also be able to view costs per business unit or per billing unit to validate showback, chargeback, or other [cloud accounting models](#).
- **Accountability:** Budgets should be established between the cloud strategy, [cloud governance](#), and [cloud adoption](#) teams based on expected adoption activities. When deviations from budget occur, the cloud strategy team and the cloud governance team must partner to quickly determine the best course of action to remediate the deviations.
- **Optimization:** During optimization efforts, the cloud strategy team can represent the investment and return value of specific workloads. If a workload has strategic value or financial impact on the business, cost-optimization efforts should be monitored closely. If there's no strategic impact on the organization and no inherent cost for poor performance of a workload, the cloud strategy team may approve over-optimization. To drive these decisions, the team must be able to view costs on a per-project scope.

## Cloud adoption team

The [cloud adoption team](#) is at the center of all adoption activities. So, they're the first line of defense against overspending. This team has an active role in all three phases of cost-consciousness.

- **Visibility:**
  - **Awareness:** It's important for the cloud adoption team to have visibility into the cost-saving goals of the effort. Simply stating that the cloud-adoption effort will help reduce costs is a recipe for failure. *Specific* visibility is important. For example, if the goal is to reduce datacenter TCO by 3 percent or annual operating expenses by 7 percent, disclose those targets early and clearly.
  - **Telemetry:** This team needs visibility into the impact of their decisions. During migration or innovation activities, their decisions have a direct effect on costs and performance. The team needs to balance these two competing factors. Performance monitoring and cost monitoring that's scoped to the team's active projects are important to provide the necessary visibility.
- **Accountability:** The cloud adoption team needs to be aware of any preset budgets that are associated with their adoption efforts. When real costs don't align with the budget, there's an opportunity to create accountability. Accountability doesn't equate to penalizing the adoption team for exceeding budget, because budget excess can result from necessary performance decisions. Instead, accountability means educating the team about the goals and how their decisions affect those goals. Additionally, accountability includes providing a dialog in which the team can communicate about decisions that led to overspending. If those decisions are misaligned with the goals of the project, this effort provides a good opportunity to partner with the cloud strategy team to make better decisions.
- **Optimization:** This effort is a balancing act, as optimization of resources can reduce the performance of the workloads that they support. Sometimes anticipated or budgeted savings can't be realized for a workload because the workload doesn't perform adequately with the budgeted resources. In those cases, the cloud adoption team has to make wise decisions and report changes to the cloud strategy team and the

cloud governance team so that budgets or optimization decisions can be corrected.

## Cloud governance team

Generally, the [cloud governance team](#) is responsible for cost management across the entire cloud-adoption effort. As outlined in the [Cost Management discipline](#) topic of the Cloud Adoption Framework's Govern methodology, cost management is the first of the Five Disciplines of Cloud Governance. Those articles outline a-series of deeper responsibilities for the cloud governance team.

This effort focuses on the following activities that are related to the development of a cost-conscious organization:

- **Visibility:** The cloud governance team works as a peer of the cloud strategy team to plan cloud-adoption budgets. These two teams also work together to regularly review actual expenses. The cloud governance team is responsible for ensuring consistent, reliable cost reporting and performance telemetry.
- **Accountability:** When budget deviations occur, the cloud strategy team and the cloud governance team must partner to quickly determine the best course of action to remediate the deviations. Generally, the cloud governance team will act on those decisions. Sometimes the action may be simple retraining for the affected [cloud adoption team](#). The cloud governance team can also help optimize deployed assets, change discounting options, or even implement automated cost-control options like blocking deployment of unplanned assets.
- **Optimization:** After assets are migrated to or created in the cloud, you can employ monitoring tools to assess performance and utilization of those assets. Proper monitoring and performance data can identify assets that should be optimized. The cloud governance team is responsible for ensuring that the monitoring and cost-reporting tools are consistently deployed. They can also help the adoption teams identify opportunities to optimize based on performance and cost telemetry.

## Cloud center of excellence

While not typically responsible for cost management, the CCoE can have a significant impact on cost-conscious organizations. Many foundational IT decisions affect costs at scale. When the CCoE does their part, costs can be reduced for multiple cloud-adoption efforts.

- **Visibility:** Any management group or resource group that houses core IT assets should be visible to the CCoE team. The team can use this data to farm opportunities to optimize.
- **Accountability:** While not typically accountable for cost, the CCoE can hold itself accountable for creating repeatable solutions that minimize cost and maximize performance.
- **Optimization:** Given the CCoE's visibility to multiple deployments, the team is in an ideal position to suggest optimization tips and to help adoption teams better tune assets.

## Next steps

Practicing these responsibilities at each level of the business helps drive a cost-conscious organization. To begin acting on this guidance, review the [organizational readiness introduction](#) to help identify the right team structures.

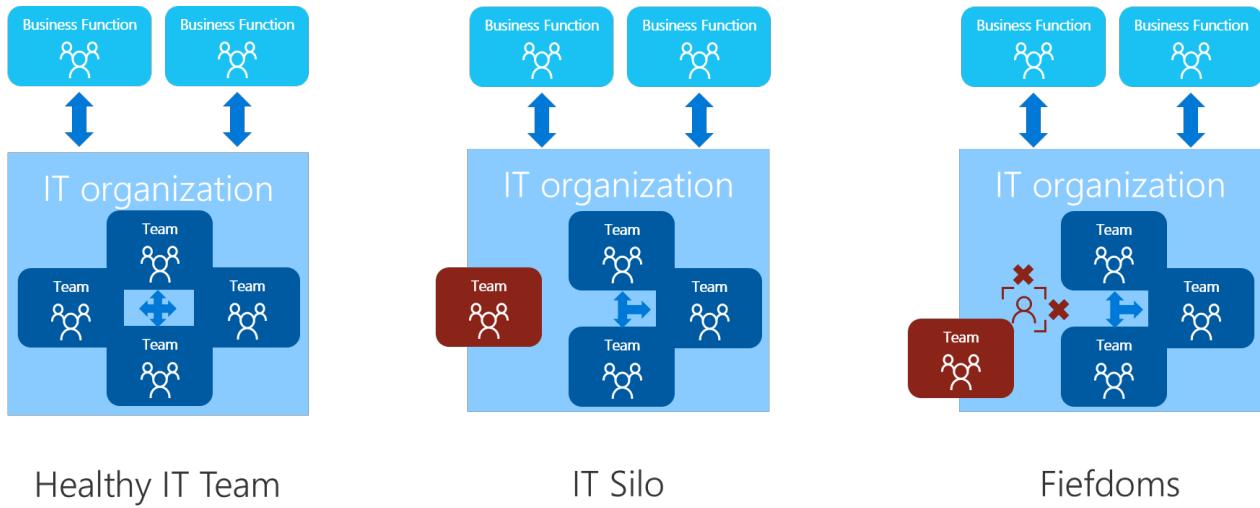
[Identify the right team structures](#)

# Organizational antipatterns: Silos and fiefdoms

11/9/2020 • 13 minutes to read • [Edit Online](#)

Success in any major change to business practices, culture, or technology operations requires a growth mindset. At the heart of the growth mindset is an acceptance of change and the ability to lead in spite of ambiguity.

Some antipatterns can block a growth mindset in organizations that want to grow and transform, including micromanagement, biased thinking, and exclusionary practices. Many of these blockers are personal challenges that create personal growth opportunities for everyone. But two common antipatterns in IT require more than individual growth or maturity: silos and fiefdoms.



These antipatterns are a result of organic changes within various teams, which result in unhealthy organizational behaviors. To address the resistance caused by each antipattern, it's important to understand the root cause of this formation.

## Healthy, organic IT teams

It's natural to create a division of labor across IT. It's healthy to establish teams that have similar expertise, shared processes, a common objective, and an aligned vision. It's also natural for those teams to have their own microculture, shared norms, and perspectives.

Healthy IT teams focus on partnering with other teams to promote the successful completion of their duties. Healthy IT teams seek to understand the business goals that their technology contribution is designed to support. The details and fiscal impact might be fuzzy, but the team's value contribution is often understood within the team.

Although healthy IT teams have a passion for the technology that they support, they're open to change and willing to try new things. Such teams are often the earliest and strongest contributors to [cloud center of excellence \(CCoE\)](#) efforts. Their contribution should be heavily encouraged.

### Natural resistance to change

At times, the microcultures within healthy IT teams might react poorly to executive or top-down decisions to drive change. This reaction is natural, as collectives of human beings with shared norms often cooperate to overcome external threats.

Changes that affect the team's day-to-day jobs, sense of security, or autonomy can be viewed as a risk to the collective. Signs of resistance are often an early indicator that the team members don't feel like they're part of the

decision-making process.

When cloud architects and other leaders invest in abolishing personal biases and driving for inclusion of the existing IT teams, this resistance is likely to lessen quickly and dissolve over time. One tool available to cloud architects and leaders to create inclusive decision making is the formation of a CCoE.

### **Healthy friction**

It's easy to confuse resistance with friction. Existing IT teams can be knowledgeable regarding past mistakes, tangible risks, tribal knowledge about solutions, and undocumented technical debt. Unfortunately, even the healthiest IT teams can fall in the trap of describing these important data points as part of a specific technical solution, which shouldn't be changed. This approach to communication masks the teams' knowledge, creating a perception of resistance.

Providing these teams with a mechanism for communicating in future-looking terminology will add data points, identify gaps, and create healthy friction around the proposed solutions. That extra friction will sand down rough edges on the solutions and drive longer-term values. Simply changing the conversation can create clarity around complex topics and generate energy to deliver more successful solutions.

The guidance on [defining corporate policy](#) is aimed at facilitating risk-based conversations with business stakeholders. But this same model can be used to facilitate conversations with teams that are perceived as cloud resistant. When the perception of resistance is widespread, it might be wise to include resistance resolution practices in the charter for a [cloud governance team](#).

## **Antipatterns**

The organic and responsive growth within IT that creates healthy IT teams can also result in antipatterns that block transformation and cloud adoption. IT silos and fiefdoms are different from the natural microcultures within healthy IT teams. In either pattern, the team focus tends to be directed toward protecting their "turf". When team members are confronted with an opportunity to drive change and improve operations, they will invest more time and energy into blocking the change than finding a positive solution.

As mentioned earlier, healthy IT teams can create natural resistance and positive friction. Silos and fiefdoms are a different challenge. There is no documented leading indicator for either antipattern. These antipatterns tend to be identified after months of [cloud center of excellence](#) and [cloud governance team](#) efforts. They're discovered as the result of ongoing resistance.

Even in toxic cultures, the efforts of the CCoE and the cloud governance team should help drive cultural growth and technical progress. After months of effort, a few teams might still show no signs of inclusive behaviors and stand firm in their resistance to change. These teams are likely operating in one of the following antipattern models: silos and fiefdoms. Although these models have similar symptoms, the root cause and approaches to addressing resistance is radically different between them.

## **IT silos**

Team members in an IT silo are likely to define themselves through their alignment to a small number of IT vendors or an area of technical specialization. But don't confuse silos with IT fiefdoms. Silos tend to be driven by comfort and passion, and silos are often easier to overcome than the fear-driven motives behind fiefdoms.

This antipattern often emerges from a common passion for a specific solution. IT silos are then reinforced by the team's advanced skills as a result of the investment in that specific solution. This superior skill can be an accelerator to cloud adoption efforts if the resistance to change can be overcome. It can also become a major blocker if the silos are broken down or if the team members can't accurately evaluate options. Fortunately, IT silos can often be overcome without any significant changes to the organizational chart.

### **Address resistance from IT silos**

IT silos can be addressed through the following approaches. The best approach will depend on the root cause of

the resistance.

**Create virtual teams:** The [organizational readiness](#) section of the Cloud Adoption Framework describes a multilayered structure for integrating and defining four virtual teams. One benefit of this structure is cross-organization visibility and inclusion. Introducing a [cloud center of excellence](#) creates a high-profile aspirational team that top engineers will want to participate in. This helps create new cross-solution alignments that aren't bound by organizational-chart constraints, and will drive inclusion of top engineers who have been sheltered by IT silos.

Introduction of a [cloud strategy team](#) will create immediate visibility to IT contributions regarding cloud adoption efforts. When IT silos fight for separation, this visibility can help motivate IT and business leaders to properly support those resistant team members. This process is a quick path to stakeholder engagement and support.

**Consider experimentation and exposure:** Team members in an IT silo have likely been constrained to think a certain way for some time. Breaking the one-track mind is a first step to addressing resistance.

Experimentation and exposure are powerful tools for breaking down barriers in silos. The team members might be resistant to competing solutions, so it's not wise to put them in charge of an experiment that competes with their existing solution. But as part of a first workload test of the cloud, the organization should implement competing solutions. The siloed team should be invited to participate as an input and review source, but not as a decision maker. This should be clearly communicated to the team, along with a commitment to engage the team more deeply as a decision maker before moving into production solutions.

During review of the competing solution, use the practices outlined in [Define corporate policy](#) to document tangible risks of the experiment and establish policies that help the siloed team become more comfortable with the future state. This will expose the team to new solutions and harden the future solution.

**Be "boundary-less":** The teams that drive cloud adoption find it easy to push boundaries by exploring exciting, new cloud-native solutions. This is one half of the approach to removing boundaries. But that thinking can further reinforce IT silos. Pushing for change too quickly and without respect to existing cultures can create unhealthy friction and lead to natural resistance.

When IT silos start to resist, it's important to be "boundary-less" in your own solutions. Be mindful of one simple truth: cloud-native isn't always the best solution. Consider hybrid solutions that might provide an opportunity to extend the existing investments of the IT silo into the future.

Also consider cloud-based versions of the solution that the IT silo team uses now. Experiment with those solutions and expose yourself to the viewpoint of those living in the IT silo. At a minimum, you will gain a fresh perspective. In many situations, you might earn enough of the IT silo's respect to lessen resistance.

**Invest in education:** Many people living in an IT silo became passionate about the current solution as a result of expanding their own education. Investing in the education of these teams is seldom misplaced. Allocate time for these individuals to engage in self-learning, classes, or even conferences to break the day-to-day focus on the current solution.

For education to be an investment, some return must come as a result of the expense. In exchange for the investment, the team might demonstrate the proposed solution to the rest of the teams involved in cloud adoption. They might also provide documentation of the tangible risks, risk management approaches, and desired policies in adopting the proposed solution. Each will engage these teams in the solution and help take advantage of their tribal knowledge.

**Turn roadblocks into speed bumps:** IT silos can slow or stop any transformation. Experimentation and iteration will find a way, but only if the project keeps moving. Focus on turning roadblocks into merely speed bumps. Define policies that everyone can be temporarily comfortable with in exchange for continued progression.

For instance, if IT security is the roadblock because its security solution can't monitor compromises of protected

data in the cloud, establish data classification policies. Prevent deployment of classified data into the cloud until an agreeable solution can be found. Invite IT security into experimentation with hybrid or cloud-native solutions to monitor protected data.

If the network team operates as a silo, identify workloads that are self-contained and don't have network dependencies. In parallel, experiment, expose, and educate the network team while working on hybrid or alternative solutions.

**Be patient and be inclusive:** It's tempting to move on without support of an IT silo. But this decision will cause disruptions and roadblocks down the road. Changing minds in members of the IT silo can take time. Be patient of their natural resistance--convert it to value. Be inclusive and invite healthy friction to improve the future solution.

**Never compete:** The IT silo exists for a reason. It persists for a reason. There is an investment in maintaining the solution that the team members are passionate about. Directly competing with the solution or the IT silo will distract from the real goal of achieving business outcomes. This trap has blocked many transformation projects.

Stay focused on the goal, as opposed to a single component of the goal. Help accentuate the positive aspects of the IT silo's solution and help the team members make wise decisions about the best solutions for the future. Don't insult or degrade the current solution, because that would be counterproductive.

**Partner with the business:** If the IT silo isn't blocking business outcomes, why do you care? There is no perfect solution or perfect IT vendor. Competition exists for a reason; each has its own benefits.

Embrace diversity and include the business by supporting and aligning to a strong [cloud strategy team](#). When an IT silo supports a solution that blocks business outcomes, it will be easier to communicate that roadblock without the noise of technical squabbles. Supporting nonblocking IT silos will show an ability to partner for the desired business outcomes. These efforts will earn more respect and greater support from the business when an IT silo presents a legitimate blocker.

## IT fiefdoms

Team members in an IT fiefdom are likely to define themselves through their alignment to a specific process or area of responsibility. The team operates under an assumption that external influence on its area of responsibility will lead to problems. Fiefdoms tend to be a fear-driven antipattern, which will require significant leadership support to overcome.

Fiefdoms are especially common in organizations that have experienced IT downsizing, frequent turbulence in IT staff, or poor IT leadership. When the business sees IT purely as a cost center, fiefdoms are much more likely to arise.

Generally, fiefdoms are the result of a line manager who fears loss of the team and the associated power base. These leaders often have a sense of duties to their team and feel a need to protect their subordinates from negative consequences. Phrases like "shelter the team from change" and "protect the team from process disruption" can be indicators of an overly guarded manager who might need more support from leadership.

### Address resistance from IT fiefdoms

IT fiefdoms can demonstrate some growth by following the approaches to [addressing IT silo resistance](#). Before you try to address resistance from an IT fiefdom, we recommend that you treat the team like an IT silo first. If those types of approaches fail to yield any significant change, the resistant team might be suffering from an IT fiefdom antipattern. The root cause of IT fiefdoms is a little more complex to address, because that resistance tends to come from the direct line manager (or a leader higher up the organizational chart). Challenges that are IT silo-driven are typically simpler to overcome.

When continued resistance from IT fiefdoms blocks cloud adoption efforts, it might be wise for a combined effort to evaluate the situation with existing IT leaders. IT leaders should carefully consider insights from the [cloud strategy team](#), [cloud center of excellence](#), and the [cloud governance team](#) before making decisions.

#### **NOTE**

IT leaders should never take changes to the organizational chart lightly. They should also validate and analyze feedback from each of the supporting teams. But transformational efforts like cloud adoption tend to magnify underlying issues that have gone unnoticed or unaddressed long before this effort. When fiefdoms are preventing the company's success, leadership changes are a likely necessity.

Fortunately, removing the leader of a fiefdom doesn't often end in termination. These strong, passionate leaders can often move into a management role after a brief period of reflection. With the right support, this change can be healthy for the leader of the fiefdom and the current team.

#### **Caution**

For managers of IT fiefdoms, protecting the team from risk is a clear leadership value. But there's a fine line between protection and isolation. When the team is blocked from participating in driving changes, it can have psychological and professional consequences on the team. The urge to resist change might be strong, especially during times of visible change.

The manager of any isolated team can best demonstrate a growth mindset by experimenting with the guidance associated with healthy IT teams in the preceding sections. Active and optimistic participation in governance and CCoE activities can lead to personal growth. Managers of IT fiefdoms are best positioned to change stifling mindsets and help the team develop new ideas.

IT fiefdoms can be a sign of systemic leadership issues. To overcome an IT fiefdom, IT leaders need the ability to make changes to operations, responsibilities, and occasionally even the people who provide line management of specific teams. When those changes are required, it's wise to approach those changes with clear and defensible data points.

Alignment with business stakeholders, business motivations, and business outcomes might be required to drive the necessary change. Partnership with the [cloud strategy team](#), [cloud center of excellence](#), and the [cloud governance team](#) can provide the data points needed for a defensible position. When necessary, these teams should be involved in a group escalation to address challenges that can't be addressed with IT leadership alone.

## Next steps

Disrupting organizational antipatterns is a team effort. To act on this guidance, review the organizational readiness introduction to identify the right team structures and participants:

[Identify the right team structures and participants](#)

# Tools and templates

11/9/2020 • 3 minutes to read • [Edit Online](#)

The Cloud Adoption Framework includes tools that help you quickly implement technical change. Use these tools, templates, and assessments to accelerate cloud adoption. The following resources can help you in each phase of adoption. Some of the tools and templates can be used in multiple phases.

## Strategy

RESOURCE	DESCRIPTION
<a href="#">Cloud journey tracker</a>	Identify your cloud adoption path based on the needs of your business.
<a href="#">Strategy and plan template</a>	Document decisions as you execute your cloud adoption strategy and plan.

## Plan

RESOURCE	DESCRIPTION
<a href="#">Cloud journey tracker</a>	Identify your cloud adoption path based on the needs of your business.
<a href="#">Strategy and plan template</a>	Document decisions, as you execute your cloud adoption strategy and plan.
<a href="#">Cloud adoption plan generator</a>	Standardize processes by deploying a backlog to <a href="#">Azure Boards</a> using a template.

## Ready

RESOURCE	DESCRIPTION
<a href="#">Readiness checklist</a>	Use this checklist to prepare your environment for adoption, including preparing your first migration landing zone, personalizing the blueprint, and expanding it.
<a href="#">Naming and tagging conventions tracking template</a>	Document decisions about naming and tagging standards to ensure consistency and reduce onboarding time.
<a href="#">CAF Foundation blueprint</a>	Use a lightweight implementation of an initial governance foundation to provide hands-on experience with governance tools in Azure.
<a href="#">CAF Migration landing zone blueprint</a>	Provision and prepare to host workloads being migrated from an on-premises environment into Azure. For more information about this blueprint, see <a href="#">Deploy a migration landing zone</a> .

RESOURCE	DESCRIPTION
Terraform modules	Open-source code base for the Terraform version of the CAF landing zones.
Terraform registry	The Terraform registry website, filtered to list all of the Cloud Adoption Framework modules needed to create a landing zone via Terraform.

## Govern

RESOURCE	DESCRIPTION
Governance benchmark assessment	Identify gaps between your current state and business priorities, and get the right resources to help you address those gaps.
CAF Foundation blueprint	Lightweight implementation of an initial governance foundation to provide hands-on experience regarding governance tools in Azure.
Governance discipline template	Define the basic set of governance processes used to enforce each governance discipline.
Cost Management discipline template	Define the policy statements and design guidance that allow you to mature the cloud governance within your organization with a focus on cost management.
Deployment Acceleration discipline template	Define the policy statements and design guidance that allow you to mature the cloud governance within your organization with a focus on deployment acceleration.
Identity Baseline discipline template	Define the policy statements and design guidance that allow you to mature the cloud governance within your organization with a focus on identity requirements.
Resource Consistency discipline template	Define the policy statements and design guidance that allow you to mature the cloud governance within your organization with a focus on resource consistency.
Security Baseline discipline template	Define the policy statements and design guidance that allow you to mature the cloud governance within your organization with a focus on security baseline.
Azure governance visualizer	The Azure governance visualizer is a PowerShell script that iterates through an Azure tenant's management group hierarchy down to the subscription level. It captures data from the most relevant Azure governance capabilities such as Azure Policy, role-based access control (RBAC), and Azure Blueprints. From the collected data, the visualizer shows your hierarchy map, creates a tenant summary, and builds granular scope insights about your management groups and subscriptions.

## Migrate

RESOURCE	DESCRIPTION
<a href="#">Datacenter migration discovery checklist</a>	Review this checklist for information that helps identify workloads, servers, and other assets in your datacenter. Use this information to help plan your migration.

## Manage

RESOURCE	DESCRIPTION
<a href="#">Microsoft Azure Well-Architected Review</a>	This online assessment will aid in defining workload specific architectures and operations options.
<a href="#">Best practices source code</a>	This deployable source code complements and accelerates adoption of best practices for Azure server management services. Use this source code to quickly enable operations management and establish an operations baseline.
<a href="#">Operations management workbook</a>	Document decisions about operations management in the cloud, and facilitate conversations with the business to ensure alignment regarding SLAs, investment in resiliency, and budget allocation related to operations.

## Organize

RESOURCE	DESCRIPTION
<a href="#">Cross-team RACI diagram</a>	Download and modify the RACI spreadsheet template to track organizational structure decisions over time.

# Azure security best practices

11/9/2020 • 26 minutes to read • [Edit Online](#)

These are the top Azure security best practices that Microsoft recommends based on lessons learned across customers and our own environments.

You can view a video presentation of these best practices in the [Microsoft Tech Community](#).

## 1. People: Educate teams about the cloud security journey

*The team needs to understand the journey they're on.*

**What:** Educate your security and IT teams on the cloud security journey and the changes they will be navigating including:

- Changes to threats in the cloud
- Shared responsibility model and how it impacts security
- Cultural and role/responsibility changes that typically accompany cloud adoption

**Why:** Moving to the cloud is a significant change that requires a shift in mindset and approach for security. While the outcomes security provides to the organization won't change, the best way to accomplish this in the cloud often changes, sometimes significantly.

In many ways, moving to the cloud is similar to moving from a standalone house into a high-rise luxury apartment building. You still have basic infrastructure (plumbing, electricity, etc.) and perform similar activities (socializing, cooking, TV and Internet, etc.) but there often quite a difference in what comes with the building (gym, restaurants, etc.), who provides and maintains them, and your daily routine.

**Who:** Everyone in the security and IT organization with any security responsibilities should be familiar with this context and the changes (from CIO/CISO to technical practitioners).

**How:** Provide teams with the context required to successfully deploy and operate during the transition to the cloud environment. Microsoft has published lessons learned by our customers and our own IT organization on their journeys to the cloud:

- [How Security Roles and Responsibilities](#) are evolving in the security organization
- [Evolution of threat environment, roles, and digital strategies](#)
- [Transformation of security, strategies, tools, and threats](#)
- [Learnings from Microsoft experience securing hyperscale cloud environment](#) that can help you on your journey

Also see the Azure Security Benchmark [GS-3: Align organization roles, responsibilities, and accountabilities](#).

## 2. People: Educate teams on cloud security technology

*People need to understand where they're going.*

**What:** Ensure your teams have time set aside for technical education on securing cloud resources including:

- Cloud technology and cloud security technology
- Recommended configurations and best practices
- Where to learn more technical details as needed

**Why:** Technical teams need access to technical information to make sound informed security decisions. Technical

teams are good at learning new technologies on the job, but the volume of details in the cloud often overwhelms their ability to fit learning into their daily routine.

Structuring dedicated time for technical learning helps ensure people have time to build confidence on their ability to assess cloud security and think through how to adapt their existing skills and processes. Even the most talented special operations teams in the military need training and intelligence to perform at their best.

**Who:** All roles that directly interact with cloud technology (in security and IT departments) should dedicate time for technical learning on cloud platforms and how to secure them.

Additionally security and IT technical managers (and often project managers) should develop familiarity with some technical details for securing cloud resources (as this will help them more effectively lead and coordinate cloud initiatives).

**How:** Ensure that technical professionals in security have time set aside for self-paced training on how to secure cloud assets. While not always feasible, ideally provide access to formal training with an experienced instructor and hands-on labs.

#### IMPORTANT

Identity protocols are critical to access control in the cloud but often not prioritized in on-premises security, so security teams should ensure to focus on developing familiarity with these protocols and logs.

Microsoft provides extensive resources to help technical professionals ramp up on securing Azure resources and report compliance:

- Azure Security
  - AZ-500 [learning path](#) (and Certification)
  - [Azure security benchmark \(ASB\)](#) –Prescriptive Best Practices and Controls for Azure Security
    - [Security Baselines for Azure](#) – Application of ASB to individual Azure Services
    - [Microsoft security best practices](#) - Videos and Documentation
- Azure Compliance
  - [Regulatory compliance](#) evaluation with Azure Security Center
- Identity Protocols and Security
  - [Azure security documentation site](#)
  - Azure AD Authentication [YouTube series](#)
  - [Securing Azure environments with Azure active directory](#)

Also see the Azure Security Benchmark [GS-3: Align organization roles, responsibilities, and accountabilities](#)

## 3. Process: Assign accountability for cloud security decisions

*If nobody is accountable for making security decisions, they won't get made.*

**What:** Designate who is responsible for making each type of security decision for the enterprise Azure environment.

**Why:** Clear ownership of security decisions speeds up cloud adoption *and* increases security. Lack of typically creates friction because nobody feels empowered to make decisions, nobody knows who to ask for a decision, and nobody is incented to research a well-informed decision. This friction frequently impedes business goals, developer timelines, IT goals, and security assurances, resulting in:

- Stalled projects that are waiting for security approval
- Insecure deployments that couldn't wait for security approval

**Who:** Security leadership designates which teams or individuals are accountable for making security decisions about the cloud.

**How:** Designate groups (or individuals) that will be responsible for making key security decisions.

Document these owners, their contact information, and socialize this widely within the security, IT, and cloud teams to ensure it's easy for all roles to contact them.

These are the typical areas where security decisions are needed, descriptions, and which teams typically make the decisions.

DECISION	DESCRIPTION	TYPICAL TEAM
Network Security	Configuration and maintenance of Azure Firewall, Network Virtual Appliances (and associated routing), WAFs, NSGs, ASGs, etc.	<i>Typically Infrastructure and endpoint security team focused on network security</i>
Network Management	Enterprise-wide virtual network and subnet allocation	<i>Typically existing network operations team in Central IT Operations</i>
Server Endpoint Security	Monitor and remediate server security (patching, configuration, endpoint security, etc.)	<i>Typically Central IT Operations and Infrastructure and endpoint security teams jointly</i>
Incident Monitoring and Response	Investigate and remediate security incidents in SIEM or source console ( Azure Security Center, Azure AD Identity Protection, etc.)	<i>Typically security operations team</i>
Policy Management	Set direction for use of Roles Based Access Control (RBAC), Azure Security Center, Administrator protection strategy, and Azure Policy to govern Azure resources	<i>Typically Policy and Standards + Security Architecture Teams jointly</i>
Identity Security and Standards	Set direction for Azure AD directories, PIM/PAM usage, MFA, password/synchronization configuration, Application Identity Standards	<i>Typically Identity and Key Management + Policy and Standards + Security Architecture Teams jointly</i>

#### NOTE

- Ensure decision makers have the appropriate education in their area of the cloud to accompany this responsibility.
- Ensure decisions are documented in policy and standards to provide a record and guide the organization over the long term.

Also see the Azure Security Benchmark [GS-3: Align organization roles, responsibilities, and accountabilities](#)

## 4. Process: Update Incident Response (IR) processes for cloud

*You don't have time to plan for a crisis during a crisis.*

**What:** Update processes and prepare analysts to for responding to security incidents on your Azure cloud platform (including any [native threat detection tools](#) you have adopted). Update processes, prepare your team, and practice with simulated attacks so they can perform at their best during incident investigation, remediation, and threat

hunting.

**Why:** Active attackers present an immediate risk to the organization that can quickly become a difficult to control situation, so you must rapidly effectively respond to attacks. This incident response (IR) process must be effective for your entire estate including all cloud platforms hosting enterprise data, systems, and accounts.

While similar in many ways, cloud platforms have important technical difference from on-premises systems that can break existing processes, typically because information is available in a different form. Security analysts may also have challenges rapidly responding to an unfamiliar environment that can slow them down (especially if they are trained only on classic on-premises architectures and network/disk forensics approaches).

**Who:** Modernizing the IR processes is typically led by [Security Operations](#) with support from other groups for knowledge and expertise.

- *Sponsorship* - This process modernization is typically sponsored by the Security Operations director or equivalent.
- *Execution* - Adapting existing processes (or writing them for the first time) is a collaborative effort involving
  - [Security Operations](#) incident management team or leadership –leads updates to process and integration of key external stakeholders including legal and communications/public relations teams
  - [Security Operations](#) security analysts – provide expertise on technical incident investigation and triage
  - [Central IT Operations](#) - Provides expertise on cloud platform (directly, via cloud center of excellence, or via external consultants)

**How:** Update processes and prepare your team so they know what to do when they find an active attacker.

- **Processes and Playbooks:** Adapt existing investigations, remediation, and threat hunting processes to the differences of how cloud platforms work (new/different tools, data sources, identity protocols, etc.).
- **Education:** Educate analysts on the overall cloud transformation, technical details of how the platform works, and new/updated processes so that they know what will be different and where to go for what they need.

**Key Focus Areas:** While there are many details described in the resource links, these are key areas to focus your education and planning efforts:

- **Shared responsibility model and cloud architectures:** To a security analyst, Azure is a software defined datacenter that provides many services including VMs (familiar) and others that are very different from on-premises such as Azure SQL Azure Functions, etc. where the best data is in the service logs or the specialized threat detection services rather than in logs for the underlying OS/VMs (which are operated by Microsoft and service multiple customers). Analysts need to understand and integrate this context into their daily workflows so they know what data to expect, where to get it, and what format it will be in.
- **Endpoint data sources:** Getting insights and data for attacks and malware on cloud hosted servers is often faster, easier, and more accurate with native cloud detection tools like Azure Security Center and EDR systems as opposed to traditional approaches of direct disk access. While direct disk forensics are available for scenarios where it is possible and required for legal proceedings ([Computer forensics in Azure](#)), this is often the most inefficient way to detect and investigate attacks.
- **Network and Identity data sources:** Many functions of cloud platforms primarily use identity primarily for access control such as access to the Azure portal (though network access controls are used extensively as well). This requires analysts to develop an understanding of cloud identity protocols to get a full, rich, picture of attacker activity (and legitimate user activity) to support incident investigation and remediation. Identity directories and protocols are also different from on-premises as they are typically based on SAML, OAuth, and OIDC and Cloud directories rather than LDAP, Kerberos, NTLM, and Active Directory that are commonly found on-premises.
- **Practice exercises:** simulated attacks and response can help build organizational muscle memory and technical readiness for your security analysts, threat hunters, incident managers, and other stakeholders in your

organization. Learning on the job and adapting is a natural part of incident response, but you should work to minimize how much you have to learn in a crisis.

#### Key Resources:

- [Incident Response Reference Guide \(IRRG\)](#)
- Guidance on [building your own security incident response process](#)
- [Azure Logging and Alerting](#)
- Microsoft Security Best Practices
  - [Transformation of Security, Strategies, Tools, & Threats](#)
  - [Security Operations](#)
- Microsoft Learnings from Cyber Defense Operations Center (CDOC)
  - [Overall Lessons Learned](#)
  - [Incident Investigation](#)
  - [Incident Remediation](#)

Also see the Azure Security Benchmark [IR-1: Preparation – update incident response process for Azure](#).

## 5. Process: Establish security posture management

*First, know thyself.*

**What:** Ensure that you are actively managing the security posture of your Azure environment by:

- Assigning clear ownership of responsibilities for
  - Monitoring security posture
  - Mitigating risks to assets
- Automating and simplifying these tasks

**Why:** Rapidly identifying and remediating common security hygiene risks significantly reduces organizational risk.

The software defined nature of cloud datacenters enables continuous monitoring of security risk (software vulnerabilities, security misconfigurations, etc.) with extensive asset instrumentation. The speed at which developers and IT team can deploy VMs, databases, and other resources also create a need to ensure resources are configured securely and actively monitored.

These new capabilities offer new possibilities, but realizing value from them requires assigning responsibility for using them. Executing consistently on rapidly evolving cloud operations also requires keeping human processes as simple and automated as possible. See the “Drive Simplicity” [security principle](#).

#### NOTE

The goal of simplification and automation isn’t about getting rid of jobs, but about removing the burden of repetitive tasks from people so they can focus on higher value human activities like engaging with and educating IT and DevOps teams.

**Who:** This is typically divided into two sets of responsibilities:

- **Security posture management** – This newer function is often an evolution of existing vulnerability management or governance functions. This includes monitoring overall security posture using Azure Security Center Secure Score and other data sources, actively working with resource owners to mitigate risks, and reporting risk to security leadership.
- **Security remediation:** Assign accountability for addressing these risks to the teams responsible for managing those resources. This should either be the DevOps teams managing their own application resources or the technology-specific teams in [Central IT Operations](#):

- **Compute and Apps Resources:**
  - App Services - Application Development/Security Team(s)
  - Containers - Application Development and/or Infrastructure/IT Operations
  - VMs/Scale sets/compute - IT/Infrastructure Operations
- **Data & Storage Resources:**
  - SQL/Redis/Data Lake Analytics/Data Lake Store - Database Team
  - Storage Accounts - Storage/Infrastructure Team
- **Identity and Access Resources:**
  - Subscriptions - Identity Team(s)
  - Key Vault – Identity or Information/Data Security Team
- **Networking Resources** - Network Security Team
- **IoT Security** - IoT Operations Team

**How:** Security is everyone's job, but not everyone currently knows how important it is, what to do, and how to do it.

- Hold resource owners accountable for the security risk just as they are held accountable for availability, performance, cost, and other success factors.
- Support resource owners with a clear understanding of why security risk matters to their assets, what they should do to mitigate risk, and how to implement it with minimal productivity loss.

#### IMPORTANT

The explanations for why, what, and how to secure resources are often similar across different resource types and applications, but it's critical to relate these to what each team already knows and cares about. Security teams should engage with their IT and DevOps counterparts as a trusted advisor and partner focused on enabling these teams to be successful.

**Tooling:** [Secure Score](#) in Azure Security Center provides an assessment of the most important security information in Azure for a wide variety of assets. This should be your starting point on posture management and can be supplemented with custom Azure policies and other mechanisms as needed.

**Frequency:** Set up a regular cadence (typically monthly) to review Azure secure score and plan initiatives with specific improvement goals. The frequency can be increased as needed.

#### TIP

Gamify the activity if possible to increase engagement, such as creating fun competitions and prizes for the DevOps teams that improve their score the most.

Also see the Azure Security Benchmark [GS-2: Define security posture management strategy](#).

## 6. Technology: Require Passwordless or Multi-Factor Authentication (MFA)

*Are you willing to bet the security of your enterprise that professional attackers can't guess or steal your admin's password?*

**What:** Require all critical impact admins to use passwordless or multi-factor authentication (MFA).

**Why:** Just as antique 'skeleton keys' won't protect a house against a modern day burglar, passwords cannot protect accounts against common attacks we see today. Technical details are described in [Your Pa\\$\\$word doesn't matter](#).

While MFA was once a burdensome extra step, Passwordless approaches today improve the logon experience using

biometric approaches like facial recognition in Windows Hello and mobile devices (where you don't have to remember or type a password). Additionally, zero trust approaches remember trusted devices, which reduce prompting for annoying out of band MFA actions (see [user sign-in frequency](#)).

**Who:** Password and multi-factor initiative is typically led by [Identity and Key Management](#) and/or [Security Architecture](#).

- *Sponsorship* - This is typically sponsored by CISO, CIO, or Director of Identity
- *Execution* - This is a collaborative effort involving
  - [Policy and standards](#) team establish clear requirements
  - [Identity and Key Management](#) or [Central IT Operations](#) to implement the policy
  - [Security Compliance management](#) monitors to ensure compliance

**How:** Implement Passwordless or MFA authentication, train administrators on how to use it (as needed), and require admins to follow using written policy. This can be accomplished by one or more of these technologies:

- [Passwordless \(Windows Hello\)](#)
- [Passwordless \(Authenticator App\)](#)
- [Azure Multifactor Authentication](#)
- Third-party MFA solution

**NOTE**

Text Message based MFA is now relatively inexpensive for attackers to bypass, so focus on passwordless & stronger MFA.

Also see the Azure Security Benchmark [ID-4: Use strong authentication controls for all Azure Active Directory based access](#).

## 7. Technology: Integrate native firewall and network security

*Simplify protection of systems and data against network attacks.*

**What:** Simplify your network security strategy and maintenance by integrating Azure Firewall, Azure Web App Firewall (WAF), and Distributed Denial of Service (DDoS) mitigations into your network security approach.

**Why:** Simplicity is critical to security as it reduces likelihood of risk from confusion, misconfigurations, and other human errors. See the "Drive Simplicity" [security principle](#).

Firewalls and WAFs are important basic security controls to protect applications from malicious traffic, but their setup and maintenance can be complex and consume a significant amount of the security team's time and attention (similar to adding custom aftermarket parts to a car). Azure's native capabilities can simplify implementation and operation of Firewalls, Web Application Firewalls, Distributed Denial of Service (DDoS) mitigations, and more.

This can free up your team's time and attention for higher value security tasks like evaluating the security of Azure Services, automating security operations, and integrating security with applications and IT solutions.

**Who:**

- *Sponsorship*: This update of network security strategy is typically sponsored by security leadership and/or IT leadership
- *Execution*: Integrating these into your cloud network security strategy is a collaborative effort involving
  - [Security Architecture](#) - Establish cloud network security architecture with cloud network and cloud network security leads.
  - [Cloud network leads \(Central IT Operations\)](#) + [Cloud Network security leads \(Infrastructure security Team\)](#)

- Establish cloud network security architecture with security architects
- Configure Firewall, NSG, and WAF capabilities and work with application architects on WAF rules
- **Application architects:** work with network security to build and refine WAF rulesets and DDoS configurations to protect the application without disrupting availability

**How:** Organizations looking to simplify their operations have two options:

- **Extend existing capabilities and architectures:** Many organizations often choose to extend the use of existing firewall capabilities so they can capitalize on existing investments into skills and process integration, particularly as they first adopt the cloud.
- **Embrace native security controls:** More and more organizations are starting to prefer using native controls to avoid the complexity of integrating third-party capabilities. These organizations are typically seeking to avoid the risk of a misconfiguration in load balancing, user-defined routes, the firewall/WAF itself, and delays in handoffs between different technical teams. This option is particularly compelling to organizations embracing infrastructure as code approaches as they can automate and instrument the built-in capabilities more easily than third-party capabilities.

Documentation on Azure native network security capabilities can be found at:

- [Azure Firewall](#)
- [Azure Web Application Firewall \(WAF\)](#)
- [Azure DDoS Protection](#)

[Azure Marketplace](#) includes many third-party firewall providers.

Also see the Azure Security Benchmark [NS-4: Protect applications and services from external network attacks](#).

## 8. Technology: Integrate native threat detection

*Simplify detection and response of attacks against Azure systems and data.*

**What:** Simplify your threat detection and response strategy by incorporating native threat detection capabilities into your security operations and SIEM.

**Why:** The purpose of security operations is to reduce the impact of active attackers who get access to the environment, as measured by mean time to acknowledge (MTTA) and remediate (MTTR) incidents. This requires both accuracy and speed in all elements of incident response, so the quality of tools and the efficiency of process execution are paramount.

It's difficult to get high threat detections using existing tools and approaches designed for on-premises threat detection because of differences in cloud technology and its rapid pace of change. Natively integrated detections provide industrial scale solutions maintained by the cloud providers that can keep up with current threats and cloud platform changes.

These native solutions also enable security operations teams to focus on incident investigation and remediation instead of wasting time trying to create alerts from unfamiliar log data, integrating tools, and maintenance tasks.

**Who:** This is typically driven by the [Security Operations](#) team.

- **Sponsorship** - This is typically sponsored by the Security Operations Director (or equivalent)..
- **Execution** – Integrating native threat detection is a collaborative effort involving those with:
  - **Security Operations:** integrate alerts into SIEM and incident investigation processes, educate analysts on cloud alerts and what they mean, and how to use the native cloud tools.
  - **Incident Preparation:** Integrate cloud incidents into practice exercises and ensure practice exercises are conducted to drive team readiness.
  - **Threat Intelligence:** Research and integrate information on cloud attacks to inform teams with context

and intelligence.

- **Security Architecture:** Integrate native tooling into security architecture documentation.
- **Policy and standards:** Set standards and policy for enabling native tooling throughout the organization. Monitor for compliance.
- **Infrastructure and Endpoint / Central IT Operations:** Configure and enable detections, integrate into automation and infrastructure as code solutions.

**How:** Enable [threat detection in Azure security center](#) for all the resources you are using and have each team integrate these into their processes as described above.

Also see the Azure Security Benchmark [LT-1: Enable threat detection for Azure resources](#).

## 9. Architecture: Standardize on a single directory and identity

*Nobody wants to deal with multiple identities and directories.*

**What:** Standardize on a single Azure AD directory and single identity for each application and user in Azure (for all enterprise identity functions).

### NOTE

This best practice refers specifically to enterprise resources. For partner accounts, use [Azure AD B2B](#) so you don't have to create and maintain accounts in your directory. For customer/citizen accounts, use [Azure AD B2C](#) to manage them.

**Why:** Multiple accounts and identity directories create unnecessary friction and confusion in daily workflows for productivity users, developers, IT and Identity Admins, security analysts, and other roles.

Managing multiple accounts and directories also creates an incentive for poor security practices such as reusing the same password across accounts and increases the likelihood of stale/abandoned accounts that attackers can target.

While it sometimes seems easier to quickly stand up a custom directory (based on LDAP, etc.) for a particular application or workload, this creates much more integration and maintenance work to set up and manage. This is similar in many ways to the decision of setting up an additional Azure tenant or additional on-premises Active Directory Forest vs. using the existing enterprise one. See also the "Drive Simplicity" [security principle](#).

**Who:** This is often a cross-team effort driven by [Security Architecture](#) or [Identity and Key Management](#) teams.

- **Sponsorship** - This is typically sponsored by [Identity and Key management](#) and [Security Architecture](#) (though some organizations may require sponsorship by CISO or CIO)
- **Execution** – This is a collaborative effort involving:
  - **Security Architecture:** Incorporates into security and IT architecture documents and diagrams
  - **Policy and standards:** Document policy and monitor for compliance
  - **Identity and Key Management** or [Central IT Operations](#) to implement the policy by enabling features and supporting developers with accounts, education, and so on.
  - **Application developers** and/or [Central IT Operations](#): Use identity in applications and Azure service configurations (responsibilities will vary based on level of DevOps adoption)

**How:** Adopt a pragmatic approach that starts with new 'greenfield' capabilities (growing today) and then clean up challenges with the 'brownfield' of existing applications and services as a follow-up exercise:

- **Greenfield:** Establish and implement a clear policy that all enterprise identity going forward should use a single Azure AD directory with a single account for each user.
- **Brownfield:** Many organizations often have multiple legacy directories and identity systems. Address these when the cost of ongoing management friction exceeds the investment to clean it up. While identity

management and synchronization solutions can mitigate some of these issues, they lack deep integration of security and productivity features that enable a seamless experience for users, admins, and developers.

The ideal time to consolidate your use of identity is during application development cycles as you:

- Modernize applications for the cloud
- Update cloud applications with DevOps processes

While there are valid reasons for a separate directory in the case of extremely independent business units or regulatory requirements, multiple directories should be avoided in all other circumstances.

Also see the Azure Security Benchmark [ID-1: Standardize Azure Active Directory as the central identity and authentication system](#).

#### IMPORTANT

The only exception to the single accounts rule is that privileged users (including IT administrators and security analysts) should have separate accounts for standard user tasks vs. administrative tasks.

For more information, see Azure Security Benchmark [Privileged Access](#).

## 10. Architecture: Use identity based access control (instead of keys)

**What:** Use Azure AD identities instead of key based authentication wherever possible (Azure Services, Applications, APIs, etc.).

**Why:** Key based authentication can be used to authenticate to cloud services and APIs but requires managing keys securely, which is challenging to perform well (especially at scale). Secure key management is difficult for non-security professionals like developers and infrastructure professionals and they often fail to do it securely, often creating major security risks for the organization.

Identity based authentication overcomes many of these challenges with mature capabilities for secret rotation, lifecycle management, administrative delegation, and more.

**Who:** This is often a cross-team effort driven by [Security Architecture](#) or [Identity and Key management](#) teams.

- *Sponsorship* - This is typically sponsored by [Security Architecture](#) or [Identity and Key management](#) (though some organizations may require sponsorship by CISO or CIO).
- *Execution* – This is a collaborative effort involving
  - **Security Architecture:** Incorporates into Security and IT Architecture diagrams and documents
  - **Policy and standards:** Document policy and monitor for compliance
  - **Identity and Key Management** or **Central IT Operations** to implement the policy by enabling features and supporting developers with accounts, education, etc.
  - **App developers** and/or **Central IT Operations:** Use identity in applications and Azure service configurations (responsibilities will vary based on level of DevOps adoption)

**How:** Setting an organizational preference and habit for using identity-based authentication requires following a process and enabling technology.

**The process:**

1. **Establish policy** and standards that clearly outline the default identity-based authentication, as well as acceptable exceptions.
2. **Educate** developers & infrastructure teams on why to use the new approach, what they need to do, and how to do it.
3. **Implement** changes in a pragmatic way – starting with new ‘greenfield’ capabilities being adopted now and in

the future (new Azure services, new applications) and then following up with a clean-up of existing 'brownfield' configurations.

#### 4. Monitor

for compliance and follow up with developer and infrastructure teams to remediate.

**The technologies:** For non-human accounts such as services or automation, use [Managed identities](#). Azure managed identities can authenticate to Azure services and resources that support Azure AD authentication. Authentication is enabled through pre-defined access grant rules, avoiding hard-coded credentials in source code or configuration files.

For services that do not support managed identities, use Azure AD to create a [Service principals](#) with restricted permissions at the resource level instead. We recommended configuring service principals with certificate credentials and fall back to client secrets. In both cases, [Azure Key Vault](#) can be used in conjunction with Azure managed identities, so that the runtime environment (such as an Azure function) can retrieve the credential from the key vault.

Also see the Azure Security Benchmark [ID-2: Manage application identities securely and automatically](#).

## 11. Architecture: Establish a single unified security strategy

*Everyone needs to row in the same direction for the boat to go forward.*

**What:** Ensure all teams are aligned to a single strategy that both enables and secures enterprise systems and data.

**Why:** When teams work in isolation without being aligned to a common strategy, their individual actions can inadvertently undermine each other's efforts, creating unnecessary friction that slows down progress against everyone's goals.

One example of this that has played out consistently in many organizations is the segmentation of assets:

- The *network security team* develops a strategy for segmenting a 'flat network' to increase security (often based on physical sites, assigned IP address ranges, or similar)
- Separately, the *identity team* developed a strategy for groups and Active Directory Organizational Units (OUs) based on their understanding and knowledge of the organization.
- *Application teams* often find it difficult to work with these systems because they were designed with limited input and understanding of business operations, goals, and risks.

In organizations where this happens, teams frequently experience conflicts over firewall exceptions, which negatively impact both security (exceptions are usually approved) and productivity (deployment is slowed for application functionality the business needs).

While security can create healthy friction by forcing critical thinking, this conflict only creates unhealthy friction that impedes goals. For more information, see [The right level of security friction](#) in the [security strategy guidance](#).

**Who:**

- **Sponsorship** - The unified strategy typically co-sponsored by CIO, CISO, and CTO (often with business leadership support for some high-level elements) and championed by representatives from each team.
- **Execution** – Security strategy must be implemented by everyone, so it should integrate input from across teams to increase ownership, buy-in, and likelihood of success.
  - **Security Architecture:** Leads the effort to build security strategy and resulting architecture, actively gather feedback from teams, and document it in presentations, documents, and diagrams for the various audiences.
  - **Policy and standards:** Captures the appropriate elements into standards and policy and then monitors for compliance.
  - **All Technical IT and security teams:** Provide input requirements, then align to and implement the enterprise strategy.

- **Application owners and developers:** Read and understand strategy documentation that applies to them (ideally, guidance tailored to their role).

#### How:

Build and implement a security strategy for cloud that includes the input and active participation of all teams. While the process documentation format will vary, this should always include:

- **Active input from teams:** Strategies typically fail if people in the organization don't buy into them. Ideally, get all teams in the same room to collaboratively build the strategy. In the workshops we conduct with customers, we often find organizations have been operating in de facto silos and these meetings often result in people meeting each other for the first time. We also find that inclusiveness is a requirement - if some teams are not invited, this meeting typically has to be repeated until all participants join it (or the project doesn't move forward).
- **Documented and communicated clearly:** All teams should have awareness of the security strategy (ideally a security component of the overall technology strategy) including why to integrate security, what is important in security, and what security success looks like. This should include specific guidance for application and development teams so they can get a clear prioritized guidance without having to read through non-relevant parts of the guidance.
- **Stable, but flexible:** Strategies should remain relatively consistent and stable, but the architectures and the documentation may need changes to add clarity and accommodate the dynamic nature of cloud. For example, filtering out malicious external traffic would stay consistent as a strategic imperative even if you shift from the use of a third-party next generation firewall to Azure firewall and adjust diagrams/guidance on how to do it.
- **Start with segmentation:** Over the course of cloud adoption, your teams will address many strategy topics large and small, but you need to start somewhere. We recommend starting the security strategy with enterprise asset segmentation as it's a foundational decision that would be challenging to change later and requires both business input and many technical teams.

Microsoft has published guidance on applying a segmentation strategy to Azure in [this video](#) and documents on [enterprise segmentation](#) and [aligning network security to it](#).

The cloud adoption framework includes guidance to help your teams with:

- **Building a cloud strategy team:** Ideally, security should be integrated into an existing cloud strategy.
- **Build or modernize a security strategy:** To meet business and security goals in the current age of cloud services and modern threats.

Also see the Azure Security Benchmark [Governance and Strategy](#).

# Architectural decision guides

11/9/2020 • 2 minutes to read • [Edit Online](#)

The architectural decision guides in the Cloud Adoption Framework describe patterns and models that help when creating cloud governance design guidance. Each decision guide focuses on one core infrastructure component of cloud deployments and lists patterns and models that can support specific cloud deployment scenarios.

When you begin to establish cloud governance for your organization, actionable governance journeys provide a baseline roadmap. These journeys make assumptions about requirements and priorities that might not reflect those of your organization.

These decision guides supplement the sample governance journeys by providing alternative patterns and models that help you align the architectural design choices made in the example design guidance with your own requirements.

## Decision guidance categories

The following categories represent foundational technologies for all cloud deployments. The sample governance journeys make design decisions related to these technologies based on the needs of example businesses, and some of these decisions might not match your organization's needs. The sections below discuss alternative options for each category, allowing you to choose a pattern or model better suited to your requirements.

**Subscriptions:** Plan your cloud deployment's subscription design and account structure to match your organization's ownership, billing, and management capabilities.

**Identity:** Integrate cloud-based identity services with your existing identity resources to support authorization and access control within your IT environment.

**Policy enforcement:** Define and enforce organizational policy rules for cloud-deployed resources and workloads that align with your governance requirements.

**Resource consistency:** Ensure that deployment and organization of your cloud-based resources align to enforce resource management and policy requirements.

**Resource tagging:** Organize your cloud-based resources to support billing models, cloud accounting approaches, management, and to optimize resource utilization and cost. Resource tagging requires a consistent and well-organized naming and metadata scheme.

**Software Defined Networking:** Deploy secure workloads to the cloud using rapid deployment and modification of virtualized networking capabilities. Software-defined networks can support agile workflows, isolate resources, and integrate cloud-based systems with your existing IT infrastructure.

**Encryption:** Secure your sensitive data using encryption to align with your organization's compliance and security policy requirements.

**Logging and reporting:** Monitor log data generated by cloud-based resources. Analyzing data provides health-related insights into the operations, maintenance, and compliance status of workloads.

## Next steps

Learn how subscriptions and accounts serve as the base of a cloud deployment.

[Subscriptions design](#)

# Subscription decision guide

11/9/2020 • 3 minutes to read • [Edit Online](#)

Effective subscription design helps organizations establish a structure to organize and manage assets in Azure during cloud adoption. This guide will help you decide when to create additional subscriptions and expand your management group hierarchy to support your business priorities.

## Prerequisites

Adopting Azure begins by creating an Azure subscription, associating it with an account, and deploying resources like virtual machines and databases to the subscription. For an overview of these concepts, see [Azure fundamental concepts](#).

- [Create your initial subscriptions](#).
- [Create additional subscriptions to scale your Azure environment](#).
- [Organize and manage your subscriptions using Azure management groups](#).

## Model your organization

Because every organization is different, Azure management groups are designed to be flexible. Modeling your cloud estate to reflect your organization's hierarchy helps you define and apply policies at higher levels of the hierarchy, and rely on inheritance to ensure that those policies are automatically applied to management groups lower in the hierarchy. Although subscriptions can be moved between different management groups, it is helpful to design an initial management group hierarchy that reflects your anticipated organizational needs.

Before finalizing your subscription design, also consider how [resource consistency](#) considerations might influence your design choices.

### NOTE

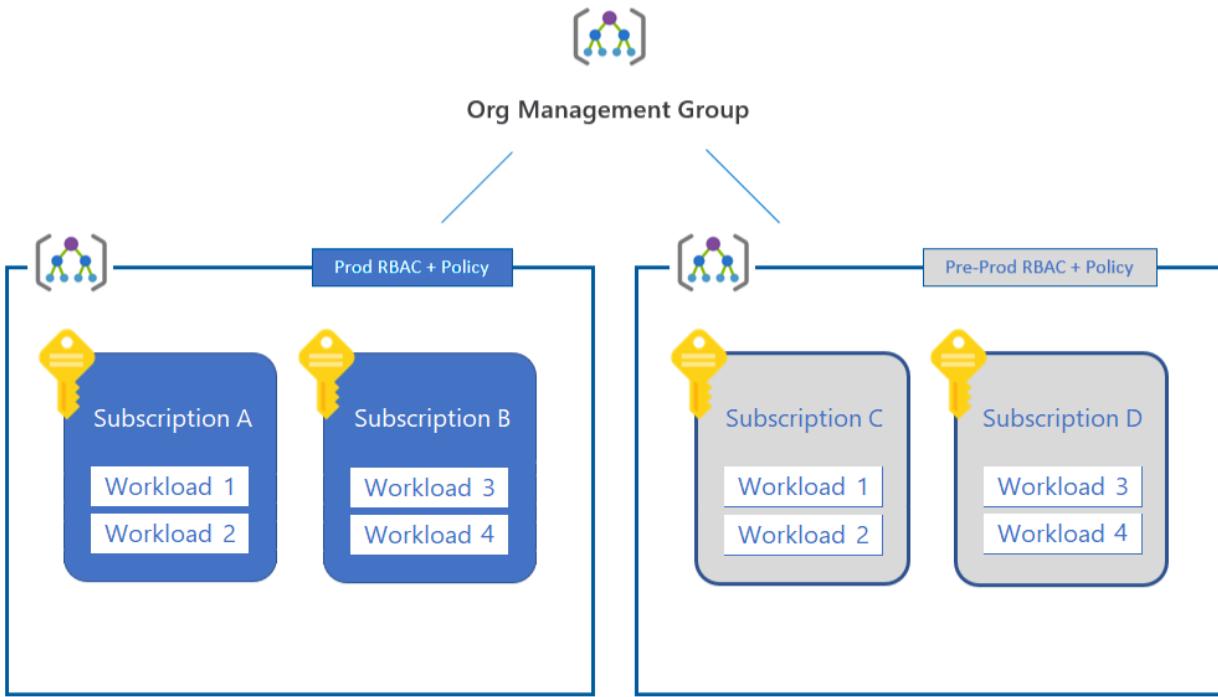
An Azure Enterprise Agreement (EA) allows you to define another organizational hierarchy for billing purposes. This hierarchy is distinct from your management group hierarchy, which focuses on providing an inheritance model for easily applying suitable policies and access control to your resources.

## Subscription design strategies

Consider the following subscription design strategies to address your business priorities.

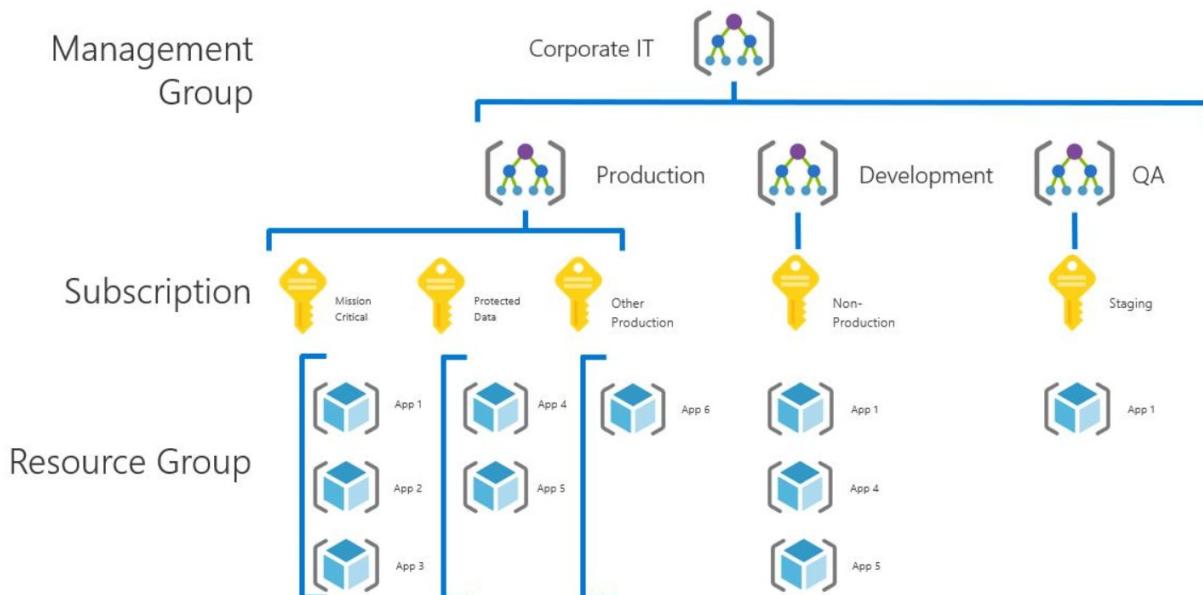
### Workload separation strategy

As an organization adds new workloads to the cloud, different ownership of subscriptions or basic separation of responsibility may result in multiple subscriptions in both the production and nonproduction management groups. While this approach does provide basic workload separation, it doesn't take significant advantage of the inheritance model to automatically apply policies across a subset of your subscriptions.



### Application category strategy

As an organization's cloud footprint grows, additional subscriptions are typically created to support applications with fundamental differences in business criticality, compliance requirements, access controls, or data protection needs. Building from the initial production and nonproduction subscriptions, the subscriptions supporting these application categories are organized under either the production or nonproduction management group as applicable. These subscriptions are typically owned and administered by the operations staff of a central IT team.



Each organization will categorize their applications differently, often separating subscriptions based on specific applications or services or along the lines of application archetypes. This categorization is often designed to support workloads that are likely to consume most of the resource limits of a subscription, or separate mission-critical workloads to ensure they don't compete with other workloads under these limits. Some workloads that might justify a separate subscription include:

- Mission-critical workloads.
- Applications that are part of cost of goods sold (COGS) within your company. For example, every widget manufactured by a company contains an Azure IoT module that sends telemetry. This may require a dedicated subscription for accounting or governance purposes as part of COGS.
- Applications subject to regulatory requirements such as HIPAA or FedRAMP.

## Functional strategy

The functional strategy organizes subscriptions and accounts along functional lines, such as finance, sales, or IT support, using a management group hierarchy.

## Business unit strategy

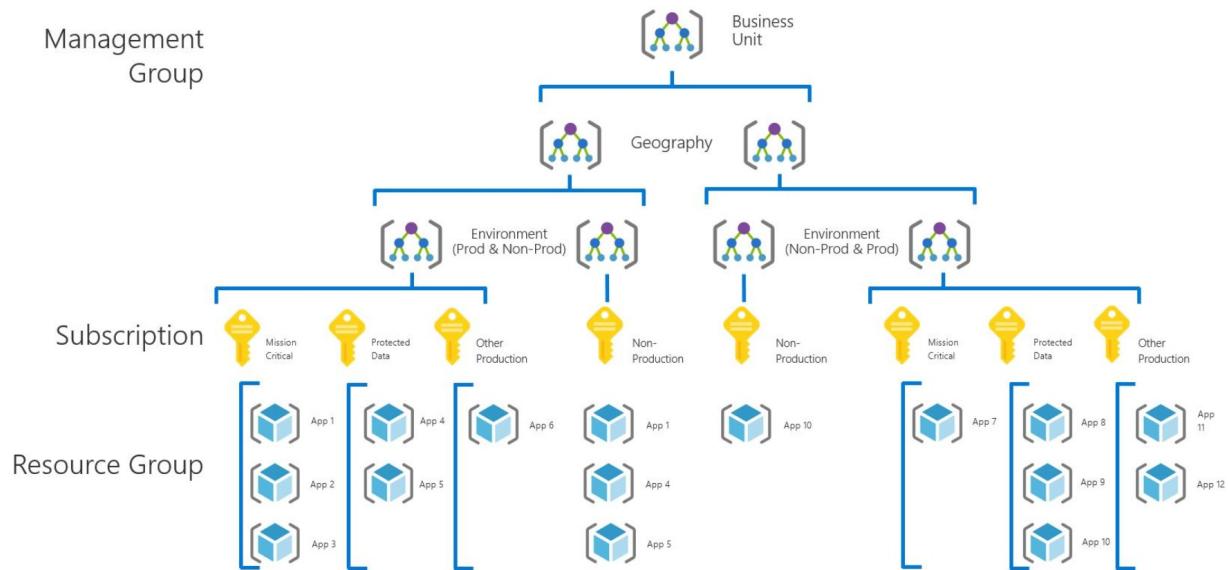
The business unit strategy groups subscriptions and accounts based on profit and loss category, business unit, division, profit center, or similar business structure using a management group hierarchy.

## Geographic strategy

For organizations with global operations, the geographic strategy groups subscriptions and accounts based on geographic regions using a management group hierarchy.

# Mix subscription strategies

Management group hierarchies can be up to six levels deep. This provides you with the flexibility to create a hierarchy that combines several of these strategies to meet your organizational needs. For example, the diagram below shows an organizational hierarchy that combines a business unit strategy with a geographic strategy.



## Related resources

- [Resource access management in Azure](#)
- [Multiple layers of governance in large enterprises](#)
- [Multiple geographic regions](#)

## Next steps

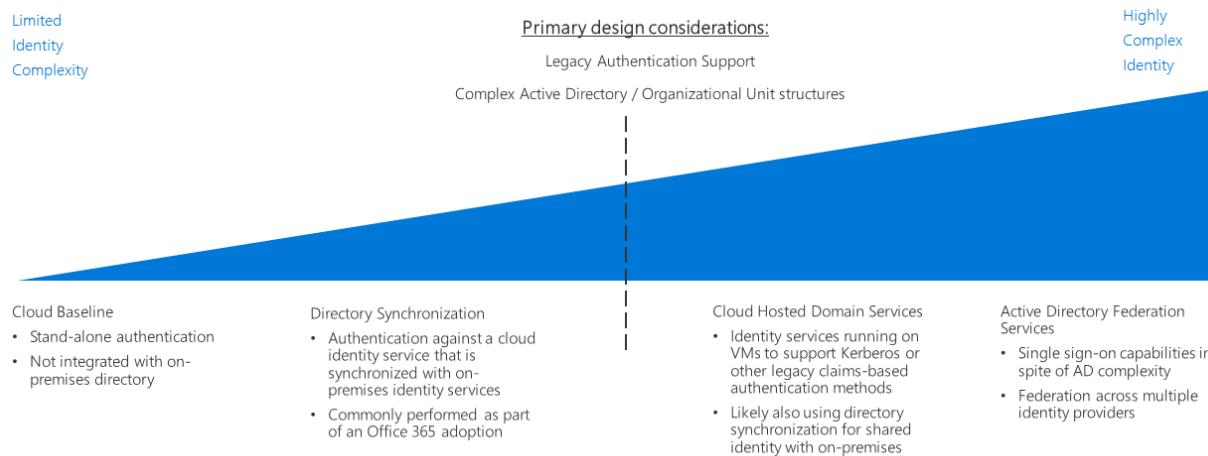
Subscription design is just one of the core infrastructure components requiring architectural decisions during a cloud adoption process. Visit the architectural decision guides overview to learn about additional strategies used when making design decisions for other types of infrastructure.

[Architectural decision guides](#)

# Identity decision guide

11/9/2020 • 7 minutes to read • [Edit Online](#)

In any environment, whether on-premises, hybrid, or cloud-only, IT needs to control which administrators, users, and groups have access to resources. Identity and access management (IAM) services enable you to manage access control in the cloud.



Jump to: [Determine identity integration requirements](#) | [Cloud baseline](#) | [Directory synchronization](#) | [Cloud-hosted domain services](#) | [Active Directory Federation Services](#) | [Learn more](#)

Several options are available for managing identity in a cloud environment. These options vary in cost and complexity. A key factor in structuring your cloud-based identity services is the level of integration required with your existing on-premises identity infrastructure.

Azure Active Directory (Azure AD) provides a base level of access control and identity management for Azure resources. If your organization's on-premises Active Directory infrastructure has a complex forest structure or customized organizational units (OUs), your cloud-based workloads might require directory synchronization with Azure AD for a consistent set of identities, groups, and roles between your on-premises and cloud environments. Additionally, support for applications that depend on legacy authentication mechanisms might require the deployment of Active Directory Domain Services (AD DS) in the cloud.

Cloud-based identity management is an iterative process. You could start with a cloud-native solution with a small set of users and corresponding roles for an initial deployment. As your migration matures, you might need to integrate your identity solution using directory synchronization or add domains services as part of your cloud deployments. Revisit your identity strategy in every iteration of your migration process.

## Determine identity integration requirements

QUESTION	CLOUD BASELINE	DIRECTORY SYNCHRONIZATION	CLOUD-HOSTED DOMAIN SERVICES	ACTIVE DIRECTORY FEDERATION SERVICES
Do you currently lack an on-premises directory service?	Yes	No	No	No

QUESTION	CLOUD BASELINE	DIRECTORY SYNCHRONIZATION	CLOUD-HOSTED DOMAIN SERVICES	ACTIVE DIRECTORY FEDERATION SERVICES
Do your workloads need to use a common set of users and groups between the cloud and on-premises environment?	No	Yes	No	No
Do your workloads depend on legacy authentication mechanisms, such as Kerberos or NTLM?	No	No	Yes	Yes
Do you require single sign-on across multiple identity providers?	No	No	No	Yes

As part of planning your migration to Azure, you will need to determine how best to integrate your existing identity management and cloud identity services. The following are common integration scenarios.

### Cloud baseline

Azure AD is the native identity and access management (IAM) system for granting users and groups access to management features on the Azure platform. If your organization lacks a significant on-premises identity solution, and you plan to migrate workloads to be compatible with cloud-based authentication mechanisms, you should begin developing your identity infrastructure using Azure AD as a base.

**Cloud baseline assumptions:** Using a purely cloud-native identity infrastructure assumes the following:

- Your cloud-based resources will not have dependencies on on-premises directory services or Active Directory servers, or workloads can be modified to remove those dependencies.
- The application or service workloads being migrated either support authentication mechanisms compatible with Azure AD or can be modified easily to support them. Azure AD relies on internet-ready authentication mechanisms such as SAML, OAuth, and OpenID Connect. Existing workloads that depend on legacy authentication methods using protocols such as Kerberos or NTLM might need to be refactored before migrating to the cloud using the cloud baseline pattern.

#### TIP

Completely migrating your identity services to Azure AD eliminates the need to maintain your own identity infrastructure, significantly simplifying your IT management.

But Azure AD is not a full replacement for a traditional on-premises Active Directory infrastructure. Directory features such as legacy authentication methods, computer management, or group policy might not be available without deploying additional tools or services to the cloud.

For scenarios where you need to integrate your on-premises identities or domain services with your cloud deployments, see the directory synchronization and cloud-hosted domain services patterns discussed below.

### Directory synchronization

For organizations with existing on-premises Active Directory infrastructure, directory synchronization is often the best solution for preserving existing user and access management while providing the required IAM

capabilities for managing cloud resources. This process continuously replicates directory information between Azure AD and on-premises directory services, allowing common credentials for users and a consistent identity, role, and permission system across your entire organization.

**NOTE**

Organizations that have adopted Microsoft 365 might have already implemented [directory synchronization](#) between their on-premises Active Directory infrastructure and Azure Active Directory.

**Directory synchronization assumptions:** Using a synchronized identity solution assumes the following:

- You need to maintain a common set of user accounts and groups across your cloud and on-premises IT infrastructure.
- Your on-premises identity services support replication with Azure AD.

**TIP**

Any cloud-based workloads that depend on legacy authentication mechanisms provided by on-premises Active Directory servers and that are not supported by Azure AD will still require either connectivity to on-premises domain services or virtual servers in the cloud environment providing these services. Using on-premises identity services also introduces dependencies on connectivity between the cloud and on-premises networks.

### Cloud-hosted domain services

If you have workloads that depend on claims-based authentication using legacy protocols such as Kerberos or NTLM, and those workloads cannot be refactored to accept modern authentication protocols such as SAML or OAuth and OpenID Connect, you might need to migrate some of your domain services to the cloud as part of your cloud deployment.

This pattern involves deploying virtual machines running Active Directory to your cloud-based virtual networks to provide Active Directory Domain Services (AD DS) for resources in the cloud. Any existing applications and services migrating to your cloud network should be able to use these cloud-hosted directory servers with minor modifications.

It's likely that your existing directories and domain services will continue to be used in your on-premises environment. In this scenario, you should also use directory synchronization to provide a common set of users and roles in both the cloud and on-premises environments.

**Cloud-hosted domain services assumptions:** Performing a directory migration assumes the following:

- Your workloads depend on claims-based authentication using protocols like Kerberos or NTLM.
- Your workload virtual machines need to be domain-joined for management or application of Active Directory group policy purposes.

**TIP**

While a directory migration coupled with cloud-hosted domain services provides great flexibility when migrating existing workloads, hosting virtual machines within your cloud virtual network to provide these services does increase the complexity of your IT management tasks. As your cloud migration experience matures, examine the long-term maintenance requirements of hosting these servers. Consider whether refactoring existing workloads for compatibility with cloud identity providers such as Azure Active Directory can reduce the need for these cloud-hosted servers.

### Active Directory Federation Services

Identity federation establishes trust relationships across multiple identity management systems to allow common authentication and authorization capabilities. You can then support single sign-on capabilities across

multiple domains within your organization or identity systems managed by your customers or business partners.

Azure AD supports federation of on-premises Active Directory domains using [Active Directory Federation Services \(AD FS\)](#). For more information about how this can be implemented in Azure, see [Extend AD FS to Azure](#).

## Learn more

For more information about identity services in Azure, see:

- [Azure AD](#). Azure AD provides cloud-based identity services. It allows you to manage access to your Azure resources and control identity management, device registration, user provisioning, application access control, and data protection.
- [Azure AD Connect](#). The Azure AD Connect tool allows you to connect Azure AD instances with your existing identity management solutions, allowing synchronization of your existing directory in the cloud.
- [Role-based access control \(RBAC\)](#). Azure AD provides RBAC to efficiently and securely manage access to resources in the management plane. Jobs and responsibilities are organized into roles, and users are assigned to these roles. RBAC allows you to control who has access to a resource along with which actions a user can perform on that resource.
- [Azure AD Privileged Identity Management \(PIM\)](#). PIM lowers the exposure time of resource access privileges and increases your visibility into their use through reports and alerts. It limits users to taking on their privileges "just in time" (JIT), or by assigning privileges for a shorter duration, after which privileges are revoked automatically.
- [Integrate on-premises Active Directory domains with Azure Active Directory](#). This reference architecture provides an example of directory synchronization between on-premises Active Directory domains and Azure AD.
- [Extend Active Directory Domain Services \(AD DS\) to Azure](#). This reference architecture provides an example of deploying AD DS servers to extend domain services to cloud-based resources.
- [Extend Active Directory Federation Services \(AD FS\) to Azure](#). This reference architecture configures Active Directory Federation Services (AD FS) to perform federated authentication and authorization with your Azure AD directory.

## Next steps

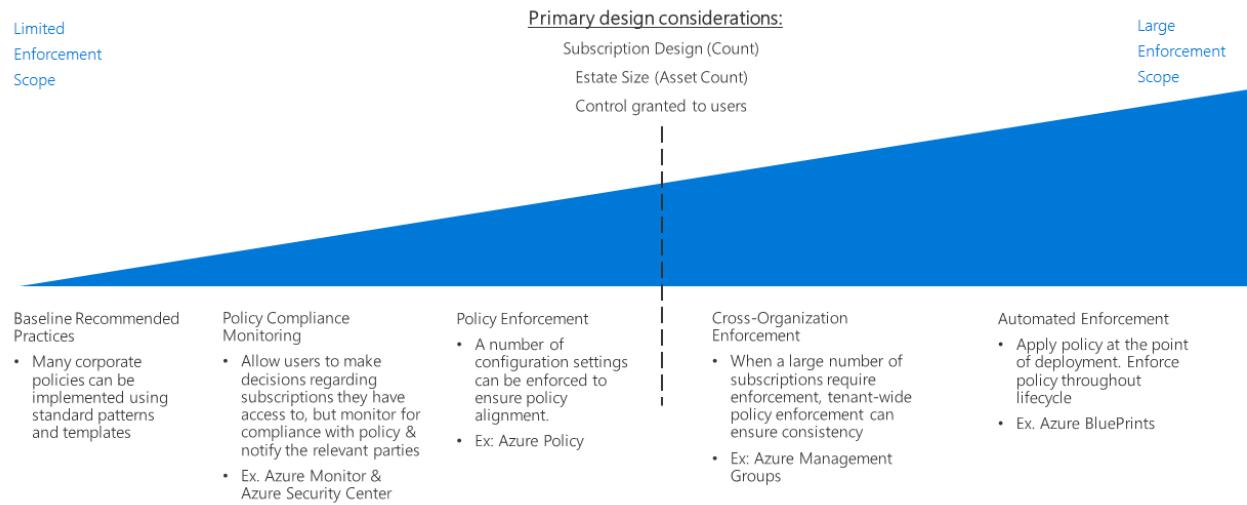
Identity is just one of the core infrastructure components requiring architectural decisions during a cloud adoption process. To learn about alternative patterns or models used when making design decisions for other types of infrastructure, see the architectural decision guides overview.

[Architectural decision guides overview](#)

# Policy enforcement decision guide

11/9/2020 • 3 minutes to read • [Edit Online](#)

Defining organizational policy is not effective unless it can be enforced across your organization. A key aspect of planning any cloud migration is determining how best to combine tools provided by the cloud platform with your existing IT processes to maximize policy compliance across your entire cloud estate.



Jump to: [Baseline best practices](#) | [Policy compliance monitoring](#) | [Policy enforcement](#) | [Cross-organization policy](#) | [Automated enforcement](#)

As your cloud estate grows, you will be faced with a corresponding need to maintain and enforce policy across a larger array of resources, and subscriptions. As your estate gets larger and your organization's policy requirements increase, the scope of your policy enforcement processes needs to expand to ensure consistent policy adherence and fast violation detection.

Platform-provided policy enforcement mechanisms at the resource or subscription level are usually sufficient for smaller cloud estates. Larger deployments justify a larger enforcement scope and may need to take advantage of more sophisticated enforcement mechanisms involving deployment standards, resource grouping and organization, and integrating policy enforcement with your logging and reporting systems.

The primary factors in determining the scope of your policy enforcement processes is your organization's [cloud governance requirements](#), the size and nature of your cloud estate, and how your organization is reflected in your [subscription design](#). An increase in size of your estate or a greater need to centrally manage policy enforcement can both justify an increase in enforcement scope.

## Baseline best practices

For single subscription and simple cloud deployments, many corporate policies can be enforced using features that are native to resources and subscriptions in Azure. The consistent use of the patterns discussed throughout the Cloud Adoption Framework [decision guides](#) can help establish a baseline level of policy compliance without specific investment in policy enforcement. These features include:

- [Deployment templates](#) can provision resources with standardized structure and configuration.
- [Tagging and naming standards](#) can help organize operations and support accounting and business requirements.
- Traffic management and networking restrictions can be implemented through [Software Defined Networking](#).

- [Role-based access control](#) can secure and isolate your cloud resources.

Start your cloud policy enforcement planning by examining how the application of the standard patterns discussed throughout these guides can help meet your organizational requirements.

## Policy compliance monitoring

A first step beyond simply relying on the policy enforcement mechanisms provided by the Azure platform is ensuring ability to verify cloud-based applications and services comply with organizational policy. This includes implementing notification capabilities for alerting responsible parties if a resource becomes noncompliant. Effective [logging and reporting](#) of the compliance status of your cloud workloads is a critical part of a corporate policy enforcement strategy.

As your cloud estate grows, additional tools such as [Azure Security Center](#) can provide integrated security and threat detection, and help apply centralized policy management and alerting for both your on-premises and cloud assets.

## Policy enforcement

In Azure, you can apply configuration settings and resource creation rules at the management group, subscription, or resource group level to help ensure policy alignment.

[Azure Policy](#) is an Azure service for creating, assigning, and managing policies. These policies enforce different rules and effects over your resources, so those resources stay compliant with your corporate standards and service-level agreements. Azure Policy evaluates your resources for noncompliance with assigned policies. For example, you might want to limit the SKU size of virtual machines in your environment. After implementing a corresponding policy, new and existing resources are evaluated for compliance. With the right policy, existing resources can be brought into compliance.

## Cross-organization policy

As your cloud estate grows to span many subscriptions that require enforcement, you will need to focus on a cloud-estate-wide enforcement strategy to ensure policy consistency.

Your [subscription design](#) must account for policy in relation to your organizational structure. In addition to helping support complex organization within your subscription design, [Azure management groups](#) can be used to assign Azure Policy rules across multiple subscriptions.

## Automated enforcement

While standardized deployment templates are effective at a smaller scale, [Azure Blueprints](#) allows large-scale standardized provisioning and deployment orchestration of Azure solutions. Workloads across multiple subscriptions can be deployed with consistent policy settings for any resources created.

For IT environments integrating cloud and on-premises resources, you may need use logging and reporting systems to provide hybrid monitoring capabilities. Your third-party or custom operational monitoring systems may offer additional policy enforcement capabilities. For larger or more mature cloud estates, consider how best to integrate these systems with your cloud assets.

## Next steps

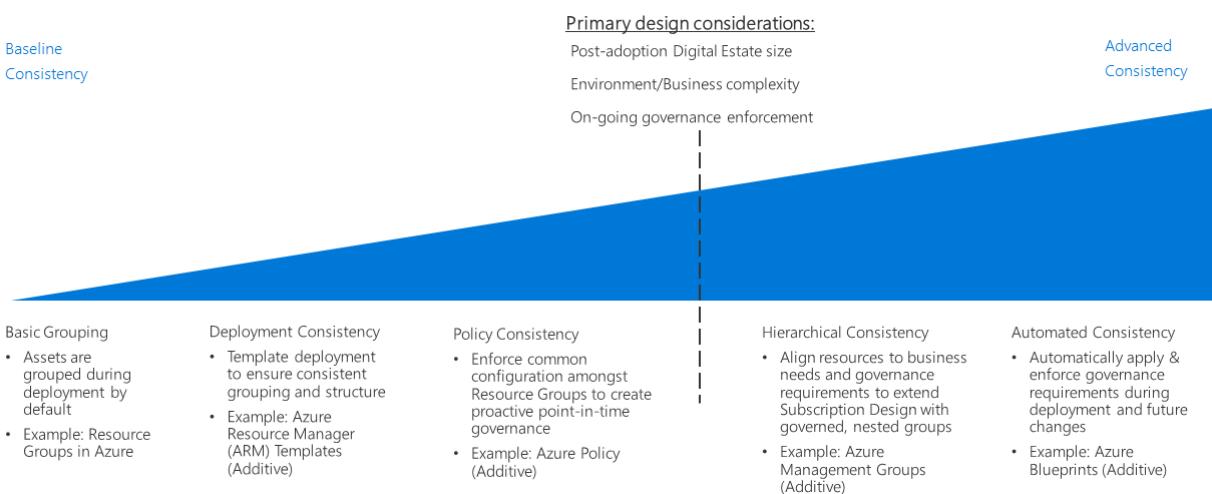
Policy enforcement is just one of the core infrastructure components requiring architectural decisions during a cloud adoption process. Visit the architectural decision guides overview to learn about alternative patterns or models used when making design decisions for other types of infrastructure.



# Resource consistency decision guide

11/9/2020 • 5 minutes to read • [Edit Online](#)

Azure [subscription design](#) defines how you organize your cloud assets in relation to your organization's structure, accounting practices, and workload requirements. In addition to this level of structure, addressing your organizational governance policy requirements across your cloud estate requires the ability to consistently organize, deploy, and manage resources within a subscription.



Jump to: [Basic grouping](#) | [Deployment consistency](#) | [Policy consistency](#) | [Hierarchical consistency](#) | [Automated consistency](#)

Decisions regarding the level of your cloud estate's resource consistency requirements are primarily driven by these factors: post-migration digital estate size, business or environmental requirements that don't fit neatly within your existing subscription design approaches, or the need to enforce governance over time after resources have been deployed.

As these factors increase in importance, the benefits of ensuring consistent deployment, grouping, and management of cloud-based resources becomes more important. Achieving more advanced levels of resource consistency to meet increasing requirements requires more effort spent in automation, tooling, and consistency enforcement, and this results in additional time spent on change management and tracking.

## Basic grouping

In Azure, [resource groups](#) are a core resource organization mechanism to logically group resources within a subscription.

Resource groups act as containers for resources with a common lifecycle as well as shared management constraints such as policy or role-based access control (RBAC) requirements. Resource groups can't be nested, and resources can only belong to one resource group. All control plane actions act on all resources in a resource group. For example, deleting a resource group also deletes all resources within that group. The preferred pattern for resource group management is to consider:

1. Are the contents of the resource group developed together?
2. Are the contents of the resource group managed, updated, and monitored together and done so by the same people or teams?
3. Are the contents of the resource group retired together?

If you answered **no** to any of the above points, the resource in question should be placed elsewhere, in another resource group.

#### IMPORTANT

Resource groups are also region specific; however, it is common for resources to be in different regions within the same resource group because they're managed together as described above. For more information about region selection, see [Multiple regions](#).

## Deployment consistency

Building on top of the base resource grouping mechanism, the Azure platform provides a system for using templates to deploy your resources to the cloud environment. You can use templates to create consistent organization and naming conventions when deploying workloads, enforcing those aspects of your resource deployment and management design.

[Azure Resource Manager templates](#) allow you to repeatedly deploy your resources in a consistent state using a predetermined configuration and resource group structure. Resource Manager templates help you define a set of standards as a basis for your deployments.

For example, you can have a standard template for deploying a web server workload that contains two virtual machines as web servers combined with a load balancer to distribute traffic between the servers. You can then reuse this template to create structurally identical set of virtual machines and load balancer whenever this type of workload is needed, only changing the deployment name and IP addresses involved.

You can also programmatically deploy these templates and integrate them with your CI/CD systems.

## Policy consistency

To ensure that governance policies are applied when resources are created, part of resource grouping design involves using a common configuration when deploying resources.

By combining resource groups and standardized Resource Manager templates, you can enforce standards for what settings are required in a deployment and what [Azure Policy](#) rules are applied to each resource group or resource.

For example, you may have a requirement that all virtual machines deployed within your subscription connect to a common subnet managed by your central IT team. You can create a standard template for deploying workload VMs to create a separate resource group for the workload and deploy the required VMs there. This resource group would have a policy rule to only allow network interfaces within the resource group to be joined to the shared subnet.

For a more in-depth discussion of enforcing your policy decisions within a cloud deployment, see [Policy enforcement](#).

## Hierarchical consistency

Resource groups allow you to support additional levels of hierarchy within your organization within the subscription, applying Azure Policy rules and access controls at a resource group level. As the size of your cloud estate grows, you may need to support more complicated cross-subscription governance requirements than can be supported using the Azure Enterprise Agreement's enterprise/department/account/subscription hierarchy.

[Azure management groups](#) allow you to organize subscriptions into more sophisticated organizational structures by grouping subscriptions in a hierarchy distinct from your Enterprise Agreement's hierarchy. This

alternate hierarchy allows you to apply access control and policy enforcement mechanisms across multiple subscriptions and the resources they contain. Management group hierarchies can be used to match your cloud estate's subscriptions with operations or business governance requirements. For more information, see the [subscription decision guide](#).

## Automated consistency

For large cloud deployments, global governance becomes both more important and more complex. It is crucial to automatically apply and enforce governance requirements when deploying resources, as well as meet updated requirements for existing deployments.

[Azure Blueprints](#) enable organizations to support global governance of large cloud estates in Azure. Blueprints move beyond the capabilities provided by standard Azure Resource Manager templates to create complete deployment orchestrations capable of deploying resources and applying policy rules. Blueprints support versioning, the ability to update all subscriptions where the blueprint was used, and the ability to lock down deployed subscriptions to avoid the unauthorized creation and modification of resources.

These deployment packages allow IT and development teams to rapidly deploy new workloads and networking assets that comply with changing organizational policy requirements. Blueprints can also be integrated into CI/CD pipelines to apply revised governance standards to deployments as they're updated.

## Next steps

Resource consistency is just one of the core infrastructure components requiring architectural decisions during a cloud adoption process. Visit the architectural decision guides overview to learn about alternative patterns or models used when making design decisions for other types of infrastructure.

[Architectural decision guides](#)

# Resource naming and tagging decision guide

11/9/2020 • 5 minutes to read • [Edit Online](#)

Organizing cloud-based resources is a crucial task for IT, unless you only have simple deployments. Use naming and tagging standards to organize your resources for these reasons:

- **Resource management:** Your IT teams will need to quickly locate resources associated with specific workloads, environments, ownership groups, or other important information. Organizing resources is critical to assigning organizational roles and access permissions for resource management.
- **Cost management and optimization:** Making business groups aware of cloud resource consumption requires IT to understand the resources and workloads each team is using. The following topics are supported by cost-related tags:
  - [Cloud accounting models](#)
  - [ROI calculations](#)
  - [Cost tracking](#)
  - [Budgets](#)
  - [Alerts](#)
  - [Recurring spend tracking and reporting](#)
  - [Post-implementation optimizations](#)
  - [Cost-optimization tactics](#)
- **Operations management:** Visibility for the operations management team regarding business commitments and SLAs is an important aspect of ongoing operations. To be well-managed, tagging for [mission criticality](#) tagging is a requirement.
- **Security:** Classification of data and security impact is a vital data point for the team, when breaches or other security issues arise. To operate securely, tagging for [data classification](#) is required.
- **Governance and regulatory compliance:** Maintaining consistency across resources helps identify deviation from agreed-upon policies. [Prescriptive guidance for resource tagging](#) demonstrates how one of the patterns below can help when deploying governance practices. Similar patterns are available to evaluate regulatory compliance using tags.
- **Automation:** In addition to making resources easier for IT to manage, a proper organizational scheme allows you to take advantage of automation as part of resource creation, operational monitoring, and the creation of DevOps processes.
- **Workload optimization:** Tagging can help identify patterns and resolve broad issues. Tag can also help identify the assets required to support a single workload. Tagging all assets associated with each workload enables deeper analysis of your mission-critical workloads to make sound architectural decisions.

## Tagging decision guide

Baseline Naming Conventions	Functional	Classification	Accounting	Partnership	Purpose
<ul style="list-style-type: none"><li>Resource naming is required for any deployment.</li><li>A standardized Naming Schema is the minimum "Tag"</li></ul>	<ul style="list-style-type: none"><li>Add tags that describe the function of the VM for easy identification</li><li>Example: Workload, Function in the workload (app, data, etc..), Environment (Dev, Staging, Prod, etc...)</li></ul>	<ul style="list-style-type: none"><li>Tags that classify the value of an asset can aid in decision making</li><li>Example: Data Classification (Public, Private, Confidential, etc...), Criticality, SLA</li></ul>	<ul style="list-style-type: none"><li>Track costs associated with asset operations</li><li>Example: Department, Project, Region, etc...</li></ul>	<ul style="list-style-type: none"><li>Align partners that count on this asset, outside of IT</li><li>Example: Owner, Owner Alias, Stakeholder, Power User, Executive</li></ul>	<ul style="list-style-type: none"><li>Aligning an asset to a business function can be valuable in making investment decisions</li><li>Example: Business Process, Business Criticality, Revenue Impact</li></ul>

Jump to: [Baseline naming conventions](#) | [Resource tagging patterns](#) | [Learn more](#)

Your tagging approach can be simple or complex, with the emphasis ranging from supporting IT teams managing cloud workloads to integrating information relating to all aspects of the business.

An IT-aligned tagging focus, such as tagging based on workload, application, function, or environment, reduces the complexity of monitoring assets and simplifies making management decisions based on operational requirements.

Tagging schemes that include a business-aligned focus, such as accounting, business ownership, or business criticality may require a larger time investment to create tagging standards that reflect business interests and maintain those standards over time. This investment yields a tagging system that provides improved accounting for costs and value of IT assets to the overall business. This association of an asset's business value to its operational cost is one of the first steps in changing the cost center perception of IT within your wider organization.

## Baseline naming conventions

A standardized naming convention is the starting point for organizing your cloud-hosted resources. A properly structured naming system allows you to quickly identify resources for both management and accounting purposes. If you have existing IT naming conventions in other parts of your organization, consider whether your cloud naming conventions should align with them or if you should establish separate cloud-based standards.

### NOTE

Naming rules and restrictions vary per Azure resource. Your naming conventions must comply with these rules.

## Resource tagging patterns

For more sophisticated organization than a consistent naming convention only can provide, cloud platforms support the ability to tag resources.

Tags are metadata elements attached to resources. Tags consist of pairs of key/value strings. The values you include in these pairs is up to you, but the application of a consistent set of global tags, as part of a comprehensive naming and tagging policy, is a critical part of an overall governance policy.

As part of your planning process, use the following questions to help determine the kind of information your resource tags need to support:

- Does your naming and tagging policies need to integrate with existing naming and organizational policies within your company?

- Will you implement a chargeback or showback accounting system? Will you need to associate resources with accounting information for departments, business groups, and teams in more detail than a simple subscription-level breakdown allows?
- Does tagging need to represent details such regulatory compliance requirements for a resource? What about operational details such as uptime requirements, patching schedules, or security requirements?
- What tags will be required for all resources based on centralized IT policy? What tags will be optional? Are individual teams allowed to implement their own custom tagging schemes?

The common tagging patterns listed below provide examples of how tagging can be used to organize cloud assets. These patterns are not meant to be exclusive and can be used in parallel, providing multiple ways of organizing assets based on your company's needs.

TAG TYPE	EXAMPLES	DESCRIPTION
Functional	<pre>app = catalogsearch1 tier = web webserver = apache env = prod env = staging env = dev</pre>	Categorize resources in relation to their purpose within a workload, what environment they've been deployed to, or other functionality and operational details.
Classification	<pre>confidentiality = private SLA = 24hours</pre>	Classifies a resource by how it is used and what policies apply to it.
Accounting	<pre>department = finance program = business-initiative region = northamerica</pre>	Allows a resource to be associated with specific groups within an organization for billing purposes.
Partnership	<pre>owner = jsmith contactalias = catsearchowners stakeholders = user1;user2;user3</pre>	Provides information about what people (outside of IT) are related or otherwise affected by the resource.
Purpose	<pre>businessprocess = support businessimpact = moderate revenueimpact = high</pre>	Aligns resources to business functions to better support investment decisions.

## Learn more

For more information about naming and tagging in Azure, see:

- [Naming conventions for Azure resources](#). Refer to this guidance for recommended naming conventions for Azure resources.
- [Use tags to organize your Azure resources and management hierarchy](#). You can apply tags in Azure at both the resource group and individual resource level, giving you flexibility in the granularity of any accounting reports based on applied tags.

## Next steps

Resource tagging is just one of the core infrastructure components requiring architectural decisions during a cloud adoption process. Visit the architectural decision guides overview to learn about alternative patterns or models used when making design decisions for other types of infrastructure.

[Architectural decision guides](#)

# Encryption decision guide

11/9/2020 • 7 minutes to read • [Edit Online](#)

Encrypting data protects it against unauthorized access. Properly implemented encryption policy provides additional layers of security for your cloud-based workloads and guards against attackers and other unauthorized users from both inside and outside your organization and networks.

Jump to: [Key management](#) | [Data encryption](#) | [Learn more](#)

Cloud encryption strategy focuses on corporate policy and compliance mandates. Encrypting resources is desirable, and many Azure services such as Azure Storage and Azure SQL Database enable encryption by default. But encryption has costs that can increase latency and overall resource usage.

For demanding workloads, striking the correct balance between encryption and performance, and determining how data and traffic is encrypted can be essential. Encryption mechanisms can vary in cost and complexity, and both technical and policy requirements can influence your decisions on how encryption is applied and how you store and manage critical secrets and keys.

Corporate policy and third-party compliance are the biggest drivers when planning an encryption strategy. Azure provides multiple standard mechanisms that can meet common requirements for encrypting data, whether at rest or in transit. For policies and compliance requirements that demand tighter controls, such as standardized secrets and key management, encryption in-use, or data-specific encryption, you'll need to develop a more sophisticated encryption strategy to support these requirements.

## Key management

Encryption of data in the cloud depends on the secure storage, management, and operational use of encryption keys. A key management system is critical to your organization's ability to create, store, and manage cryptographic keys, as well as important passwords, connection strings, and other IT confidential information.

Modern key management systems such as Azure Key Vault support storage and management of software protected keys for dev and test usage and hardware security module (HSM) protected keys for maximum protection of production workloads or sensitive data.

When planning a cloud migration, the following table can help you decide how to store and manage encryption keys, certificates, and secrets that are critical for creating secure and manageable cloud deployments:

QUESTION	CLOUD-NATIVE	BRING YOUR OWN KEY	HOLD YOUR OWN KEY
Does your organization lack centralized key and secret management?	Yes	No	No
Will you need to limit the creation of keys and secrets to devices to your on-premises hardware, while using these keys in the cloud?	No	Yes	No

QUESTION	CLOUD-NATIVE	BRING YOUR OWN KEY	HOLD YOUR OWN KEY
Does your organization have rules or policies in place that would prevent keys from being stored offsite?	No	No	Yes

## Cloud-native

With cloud-native key management, all keys and secrets are generated, managed, and stored in a cloud-based vault such as Azure Key Vault. This approach simplifies many IT tasks related to key management, such as key backup, storage, and renewal.

**Cloud-native assumptions:** Using a cloud-native key management system includes these assumptions:

- You trust the cloud key management solution with creating, managing, and hosting your organization's secrets and keys.
- You enable all on-premises applications and services that rely on accessing encryption services or secrets to access the cloud key management system.

## Bring your own key (BYOK)

With a BYOK approach, you generate keys on dedicated HSM hardware within your on-premises environment, then securely transferring these keys to a cloud-based management system such as Azure Key Vault for use with your cloud-hosted resources.

**Bring-your-own-key assumptions:** Generating keys on-premises and using them with a cloud-based key management system includes these assumptions:

- You trust the underlying security and access control infrastructure of the cloud platform for hosting and using your keys and secrets.
- Your cloud-hosted applications or services can access and use keys and secrets in a robust and secure way.
- You're required by regulatory or organizational policy to keep the creation and management of your organization's secrets and keys on-premises.

## On-premises (hold your own key)

Certain scenarios might have regulatory, policy, or technical reasons prohibiting the storage of keys on a cloud-based key management system. If so, you must generate keys using on-premises hardware, store and manage them using an on-premises key management system, and establish a way for cloud-based resources to access these keys for encryption purposes. Note that holding your own key might not be compatible with all Azure-based services.

**On-premises key management assumptions:** Using an on-premises key management system includes these assumptions:

- You're required by regulatory or organizational policy to keep the creation, management, and hosting of your organization's secrets and keys on-premises.
- Any cloud-based applications or services that rely on accessing encryption services or secrets can access the on-premises key management system.

## Data encryption

Consider several different states of data with different encryption needs when planning your encryption policy:

DATA STATE	DATA
Data in transit	Internal network traffic, internet connections, connections between datacenters or virtual networks
Data at rest	Databases, files, virtual drives, PaaS storage
Data in use	Data loaded in RAM or in CPU caches

## Data in transit

Data in transit is data moving between resources on the internal, between datacenters or external networks, or over the internet.

Data in transit is usually encrypted by requiring SSL/TLS protocols for network traffic. Always encrypt traffic between your cloud-hosted resources and external networks or the public internet. PaaS resources typically enforce SSL/TLS encryption by default. Your cloud adoption teams and workload owners should consider enforcing encryption for traffic between IaaS resources hosted inside your virtual networks.

**Assumptions about encrypting data in transit:** Implementing proper encryption policy for data in transit assumes the following:

- All publicly accessible endpoints in your cloud environment will communicate with the public internet using SSL/TLS protocols.
- When connecting cloud networks with on-premises or other external network over the public internet, use encrypted VPN protocols.
- When connecting cloud networks with on-premises or other external network using a dedicated WAN connection such as ExpressRoute, you will use a VPN or other encryption appliance on-premises paired with a corresponding virtual VPN or encryption appliance deployed to your cloud network.
- If you have sensitive data that shouldn't be included in traffic logs or other diagnostics reports visible to IT staff, you will encrypt all traffic between resources in your virtual network.

## Data at rest

Data at rest represents any data not being actively moved or processed, including files, databases, virtual machine drives, PaaS storage accounts, or similar assets. Encrypting stored data protects virtual devices or files against unauthorized access either from external network penetration, rogue internal users, or accidental releases.

PaaS storage and database resources generally enforce encryption by default. IaaS resources can be secured by encrypting data at the virtual disk level or by encrypting the entire storage account hosting your virtual drives. All of these assets can make use of either Microsoft-managed or customer-managed keys stored in Azure Key Vault.

Encryption for data at rest also encompasses more advanced database encryption techniques, such as column-level and row level encryption, providing much more control over exactly what data is being secured.

Your overall policy and compliance requirements, the sensitivity of the data being stored, and the performance requirements of your workloads should determine which assets require encryption.

## Assumptions about encrypting data at rest

Encrypting data at rest assumes the following:

- You're storing data that is not meant for public consumption.
- Your workloads can accept the added latency cost of disk encryption.

## Data in use

Encryption for data in use involves securing data in nonpersistent storage, such as RAM or CPU caches. Use of technologies such as full memory encryption, enclave technologies, such as Intel's Secure Guard Extensions (SGX).

This also includes cryptographic techniques, such as homomorphic encryption that can be used to create secure, trusted execution environments.

**Assumptions about encrypting data in use:** Encrypting data in use assumes the following:

- You're required to maintain data ownership separate from the underlying cloud platform at all times, even at the RAM and CPU level.

## Learn more

For more information about encryption and key management in Azure, see:

- [Azure encryption overview](#): A detailed description of how Azure uses encryption to secure both data at rest and data in transit.
- [Azure Key Vault](#): Key Vault is the primary key management system for storing and managing cryptographic keys, secrets, and certificates within Azure.
- [Azure data security and encryption best practices](#): A discussion of Azure data security and encryption best practices.
- [Confidential computing in Azure](#): Azure's confidential computing initiative provides tools and technology to create trusted execution environments or other encryption mechanisms to secure data in use.

## Next steps

Encryption is just one of the core infrastructure components requiring architectural decisions during a cloud adoption process. To learn about alternative patterns or models used when making design decisions for other types of infrastructure, see the architectural decision guides overview.

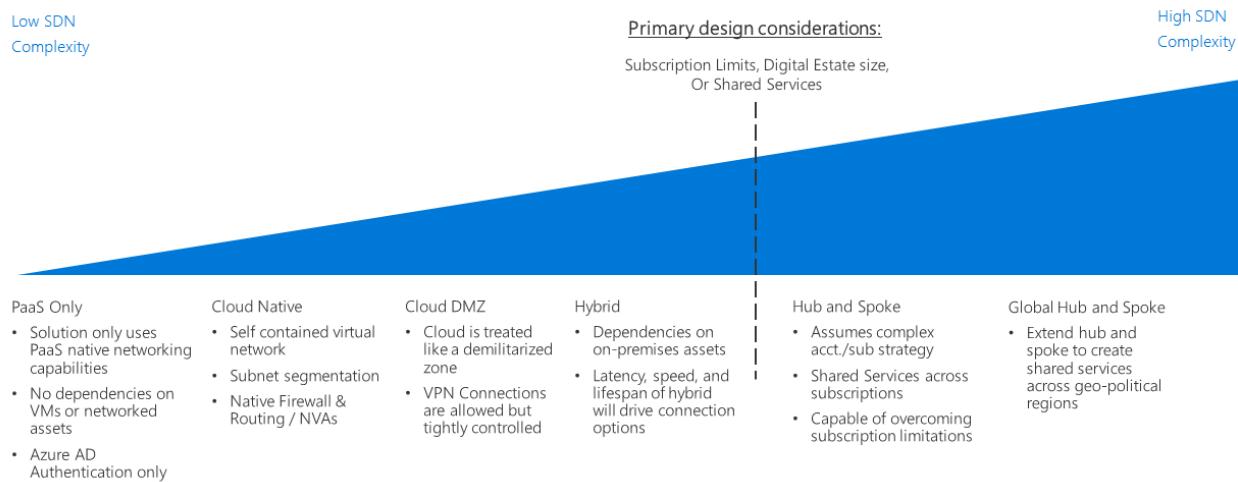
[Architectural decision guides overview](#)

# Software Defined Networking decision guide

11/9/2020 • 3 minutes to read • [Edit Online](#)

Software Defined Networking (SDN) is a network architecture designed to allow virtualized networking functionality that can be centrally managed, configured, and modified through software. SDN enables the creation of cloud-based networks using the virtualized equivalents to physical routers, firewalls, and other networking devices used in on-premises networks. SDN is critical to creating secure virtual networks on public cloud platforms such as Azure.

## Networking decision guide



Jump to: [PaaS only](#) | [Cloud-native](#) | [Cloud DMZ](#) | [Hybrid](#) | [Hub and spoke model](#) | [Learn more](#)

SDN provides several options with varying degrees of pricing and complexity. The above discovery guide provides a reference to quickly personalize these options to best align with specific business and technology strategies.

The inflection point in this guide depends on several key decisions that your cloud strategy team has made before making decisions about networking architecture. Most important among these are decisions involving your [digital estate definition](#) and [subscription design](#), which may also require inputs from decisions made related to your cloud accounting and global markets strategies.

Small single-region deployments of fewer than 1,000 VMs are less likely to be significantly affected by this inflection point. Conversely, large adoption efforts with more than 1,000 VMs, multiple business units, or multiple geopolitical markets, could be substantially affected by your SDN decision and this key inflection point.

## Choose the right virtual networking architectures

This section expands on the decision guide to help you choose the right virtual networking architectures.

There are many ways to implement SDN technologies to create cloud-based virtual networks. How you structure the virtual networks used in your migration and how those networks interact with your existing IT infrastructure will depend on a combination of the workload requirements and your governance requirements.

When planning which virtual networking architecture or combination of architectures to consider when planning your cloud migration, consider the following questions to help determine what's right for your organization:

QUESTION	PAAS-ONLY	CLOUD-NATIVE	CLOUD DMZ	HYBRID	HUB AND SPOKE
Will your workload only use PaaS services and not require networking capabilities beyond those provided by the services themselves?	Yes	No	No	No	No
Does your workload require integration with on-premises applications?	No	No	Yes	Yes	Yes
Have you established mature security policies and secure connectivity between your on-premises and cloud networks?	No	No	No	Yes	Yes
Does your workload require authentication services not supported through cloud identity services, or do you need direct access to on-premises domain controllers?	No	No	No	Yes	Yes
Will you need to deploy and manage a large number of VMs and workloads?	No	No	No	No	Yes
Will you need to provide centralized management and on-premises connectivity while delegating control over resources to individual workload teams?	No	No	No	No	Yes

# Virtual networking architectures

Learn more about the primary Software Defined Networking architectures:

- **PaaS-only:** Most platform as a service (PaaS) products support a limited set of built-in networking features and may not require an explicitly defined software defined network to support workload requirements.
- **Cloud-native:** A cloud-native architecture supports cloud-based workloads using virtual networks built on the cloud platform's default Software Defined Networking capabilities, without reliance on on-premises or other external resources.
- **Cloud DMZ:** Supports limited connectivity between your on-premises and cloud networks, secured through the implementation of a perimeter network tightly controlling traffic between the two environments.
- **Hybrid:** The hybrid cloud network architecture allows virtual networks in trusted cloud environments to access your on-premises resources and vice versa.
- **Hub and spoke:** The hub and spoke architecture allows you to centrally manage external connectivity and shared services, isolate individual workloads, and overcome potential subscription limits.

## Learn more

For more information about Software Defined Networking in Azure, see:

- [Azure Virtual Network](#). On Azure, the core SDN capability is provided by Azure Virtual Network, which acts as a cloud analog to physical on-premises networks. Virtual networks also act as a default isolation boundary between resources on the platform.
- [Azure best practices for network security](#). Recommendations from the Azure security team on how to configure your virtual networks to minimize security vulnerabilities.

## Next steps

Software Defined Networking is just one of the core infrastructure components requiring architectural decisions during a cloud adoption process. Visit the architectural decision guides overview to learn about alternative patterns or models used when making design decisions for other types of infrastructure.

[Architectural decision guides](#)

# Software Defined Networking: PaaS-only

11/9/2020 • 2 minutes to read • [Edit Online](#)

When you implement a platform as a service (PaaS) resource, the deployment process automatically creates an assumed underlying network with a limited number of controls over that network, including load balancing, port blocking, and connections to other PaaS services.

In Azure, several PaaS resource types can be [deployed into a virtual network](#) or [connected to a virtual network](#), integrating these resources with your existing virtual networking infrastructure. Other services, such as [App Service Environment](#), [Azure Kubernetes Service \(AKS\)](#), and [Service Fabric](#) must be deployed within a virtual network. In many cases, a PaaS-only networking architecture, relying solely on the default native networking capabilities provided by PaaS resources, is sufficient to meet a workload's connectivity and traffic management requirements.

If you're considering a PaaS only networking architecture, be sure you validate that the required assumptions align with your requirements.

## PaaS-only assumptions

Deploying a PaaS-only networking architecture assumes the following:

- The application being deployed is a standalone application or depends only on other PaaS resources that do not require a virtual network.
- Your IT operations teams can update their tools, training, and processes to support management, configuration, and deployment of standalone PaaS applications.
- The PaaS application is not part of a broader cloud migration effort that will include IaaS resources.

These assumptions are minimum qualifiers aligned to deploying a PaaS-only network. While this approach may align with the requirements of a single application deployment, each cloud adoption team should consider these long-term questions:

- Will this deployment expand in scope or scale to require access to other non-PaaS resources?
- Are other PaaS deployments planned beyond the current solution?
- Does the organization have plans for other future cloud migrations?

The answers to these questions would not preclude a team from choosing a PaaS only option but should be considered before making a final decision.

# Software Defined Networking: Cloud-native

11/9/2020 • 2 minutes to read • [Edit Online](#)

A cloud-native virtual network is required when deploying IaaS resources such as virtual machines to a cloud platform. Access to virtual networks from external sources, similar to the web, need to be explicitly provisioned. These types of virtual networks support the creation of subnets, routing rules, and virtual firewall and traffic management devices.

A cloud-native virtual network has no dependencies on your organization's on-premises or other non-cloud resources to support the cloud-hosted workloads. All required resources are provisioned either in the virtual network itself or by using managed PaaS offerings.

## Cloud-native assumptions

Deploying a cloud-native virtual network assumes the following:

- The workloads you deploy to the virtual network have no dependencies on applications or services that are accessible only from inside your on-premises network. Unless they provide endpoints accessible over the public internet, applications and services hosted internally on-premises are not usable by resources hosted on a cloud platform.
- Your workload's identity management and access control depends on the cloud platform's identity services or IaaS servers hosted in your cloud environment. You will not need to directly connect to identity services hosted on-premises or other external locations.
- Your identity services do not need to support single sign-on (SSO) with on-premises directories.

Cloud-native virtual networks have no external dependencies. This makes them simple to deploy and configure, and as a result this architecture is often the best choice for experiments or other smaller self-contained or rapidly iterating deployments.

Additional issues your cloud adoption teams should consider when discussing a cloud-native virtual networking architecture include:

- Existing workloads designed to run in an on-premises datacenter may need extensive modification to take advantage of cloud-based functionality, such as storage or authentication services.
- Cloud-native networks are managed solely through the cloud platform management tools, and therefore may lead to management and policy divergence from your existing IT standards as time goes on.

## Next steps

For more information about cloud-native virtual networking in Azure, see:

- [Azure Virtual Network guides](#): Newly created virtual networks are cloud-native by default. Use these guides to help plan the design and deployment of your virtual networks.
- [Azure networking limits](#): Each virtual network and connected resources exists in a single subscription. These resources bound by subscription limits.

# Software Defined Networking: Cloud DMZ

11/9/2020 • 2 minutes to read • [Edit Online](#)

The Cloud DMZ network architecture allows limited access between your on-premises and cloud-based networks, using a virtual private network (VPN) to connect the networks. Although a DMZ model is commonly used when you want to secure external access to a network, the Cloud DMZ architecture discussed here is intended specifically to secure access to the on-premises network from cloud-based resources and vice versa.

This architecture is designed to support scenarios where your organization wants to start integrating cloud-based workloads with on-premises workloads but may not have fully matured cloud security policies or acquired a secure dedicated WAN connection between the two environments. As a result, cloud networks should be treated like a DMZ to ensure on-premises services are secure.

The DMZ deploys network virtual appliances (NVAs) to implement security functionality such as firewalls and packet inspection. Traffic passing between on-premises and cloud-based applications or services must pass through the DMZ where it can be audited. VPN connections and the rules determining what traffic is allowed through the DMZ network are strictly controlled by IT security teams.

## Cloud DMZ assumptions

Deploying a Cloud DMZ includes the following assumptions:

- Your security teams have not fully aligned on-premises and cloud-based security requirements and policies.
- Your cloud-based workloads require access to limited subset of services hosted on your on-premises or third-party networks, or users or applications in your on-premises environment need limited access to cloud-hosted resources.
- Implementing a VPN connection between your on-premises networks and cloud provider is not prevented by corporate policy, regulatory requirements, or technical compatibility issues.
- Your workloads either do not require multiple subscriptions to bypass subscription resource limits, or they involve multiple subscriptions but don't require central management of connectivity or shared services used by resources spread across multiple subscriptions.

Your cloud adoption teams should consider the following issues when looking at implementing a Cloud DMZ virtual networking architecture:

- Connecting on-premises networks with cloud networks increases the complexity of your security requirements. Even though connections between cloud networks and the on-premises environment are secured, you still need to ensure cloud resources are secured. Any public IPs created to access cloud-based workloads need to be properly secured using a [public-facing DMZ](#) or [Azure Firewall](#).
- The Cloud DMZ architecture is commonly used as a stepping stone while connectivity is further secured and security policy aligned between on-premises and cloud networks, allowing a broader adoption of a full-scale hybrid networking architecture. It may also apply to isolated deployments with specific security, identity, and connectivity needs that the Cloud DMZ approach satisfies.

## Learn more

For more information about implementing a Cloud DMZ in Azure, see:

- [Implement a DMZ between Azure and your on-premises datacenter](#). This article discusses how to implement a

secure hybrid network architecture in Azure.

# Software Defined Networking: Hybrid network

11/9/2020 • 2 minutes to read • [Edit Online](#)

The hybrid cloud network architecture allows virtual networks to access your on-premises resources and services and vice versa, using a dedicated WAN connection such as ExpressRoute or other connection method to directly connect the networks.

Building on the cloud-native virtual network architecture, a hybrid virtual network is isolated when initially created. Adding connectivity to the on-premises environment grants access to and from the on-premises network, although all other inbound traffic targeting resources in the virtual network need to be explicitly allowed. You can secure the connection using virtual firewall devices and routing rules to limit access or you can specify exactly what services can be accessed between the two networks using cloud-native routing features or deploying network virtual appliances (NVAs) to manage traffic.

Although the hybrid networking architecture supports VPN connections, dedicated WAN connections like ExpressRoute are preferred due to higher performance and increased security.

## Hybrid assumptions

Deploying a hybrid virtual network includes the following assumptions:

- Your IT security teams have aligned on-premises and cloud-based network security policy to ensure cloud-based virtual networks can be trusted to communicate directly with on-premises systems.
- Your cloud-based workloads require access to storage, applications, and services hosted on your on-premises or third-party networks, or your users or applications in your on-premises need access to cloud-hosted resources.
- You need to migrate existing applications and services that depend on on-premises resources, but don't want to expend the resources on redevelopment to remove those dependencies.
- Connecting your on-premises networks to cloud resources over VPN or dedicated WAN is not prevented by corporate policy, data sovereignty requirements, or other regulatory compliance issues.
- Your workloads either do not require multiple subscriptions to bypass subscription resource limits, or your workloads involve multiple subscriptions but do not require central management of connectivity or shared services used by resources spread across multiple subscriptions.

Your cloud adoption teams should consider the following issues when looking at implementing a hybrid virtual networking architecture:

- Connecting on-premises networks with cloud networks increases the complexity of your security requirements. Both networks must be secured against external vulnerabilities and unauthorized access from both sides of the hybrid environment.
- Scaling the number and size of workloads within a hybrid cloud environment can add significant complexity to routing and traffic management.
- You will need to develop compatible management and access control policies to maintain consistent governance throughout your organization.

## Learn more

For more information about hybrid networking in Azure, see:

- [Hybrid network reference architecture](#). Azure hybrid virtual networks use either an ExpressRoute circuit or Azure VPN to connect your virtual network with your organization's existing IT assets not hosted in Azure. This article discusses the options for creating a hybrid network in Azure.

# Software Defined Networking: Hub and spoke

11/9/2020 • 2 minutes to read • [Edit Online](#)

The hub and spoke networking model organizes your Azure-based cloud network infrastructure into multiple connected virtual networks. This model allows you to more efficiently manage common communication or security requirements and deal with potential subscription limitations.

In the hub and spoke model, the *hub* is a virtual network that acts as a central location for managing external connectivity and hosting services used by multiple workloads. The *spokes* are virtual networks that host workloads and connect to the central hub through [virtual network peering](#).

All traffic passing in or out of the workload spoke networks is routed through the hub network where it can be routed, inspected, or otherwise managed by centrally managed IT rules or processes.

This model aims to address the following concerns:

- **Cost savings and management efficiency.** Centralizing services that can be shared by multiple workloads, such as network virtual appliances (NVAs) and DNS servers, in a single location allows IT to minimize redundant resources and management effort across multiple workloads.
- **Overcoming subscription limits.** Large cloud-based workloads may require the use of more resources than are allowed within a single Azure subscription. Peering workload virtual networks from different subscriptions to a central hub can overcome these limits. For more information, see [Azure networking limits](#).
- **Separation of concerns.** The ability to deploy individual workloads between central IT teams and workload teams.

The following diagram shows an example hub and spoke architecture including centrally managed hybrid connectivity.



The hub and spoke architecture is often used alongside the hybrid networking architecture, providing a centrally managed connection to your on-premises environment shared between multiple workloads. In this scenario, all traffic traveling between the workloads and on-premises passes through the hub where it can be managed and secured.

## Hub and spoke assumptions

Implementing a hub and spoke virtual networking architecture assumes the following:

- Your cloud deployments will involve workloads hosted in separate working environments, such as development, test, and production, that all rely on a set of common services such as DNS or directory services.
- Your workloads do not need to communicate with each other but have common external communications and shared services requirements.
- Your workloads require more resources than are available within a single Azure subscription.
- You need to provide workload teams with delegated management rights over their own resources while maintaining central security control over external connectivity.

## Global hub and spoke

Hub and spoke architectures are commonly implemented with virtual networks deployed to the same Azure region to minimize latency between networks. Large organizations with a global presence might need to deploy workloads across multiple regions for availability, disaster recovery, or regulatory requirements. The hub and

spoke model can use of Azure [global virtual network peering](#) to extend centralized management and shared services across regions and support workloads distributed across the world.

## Learn more

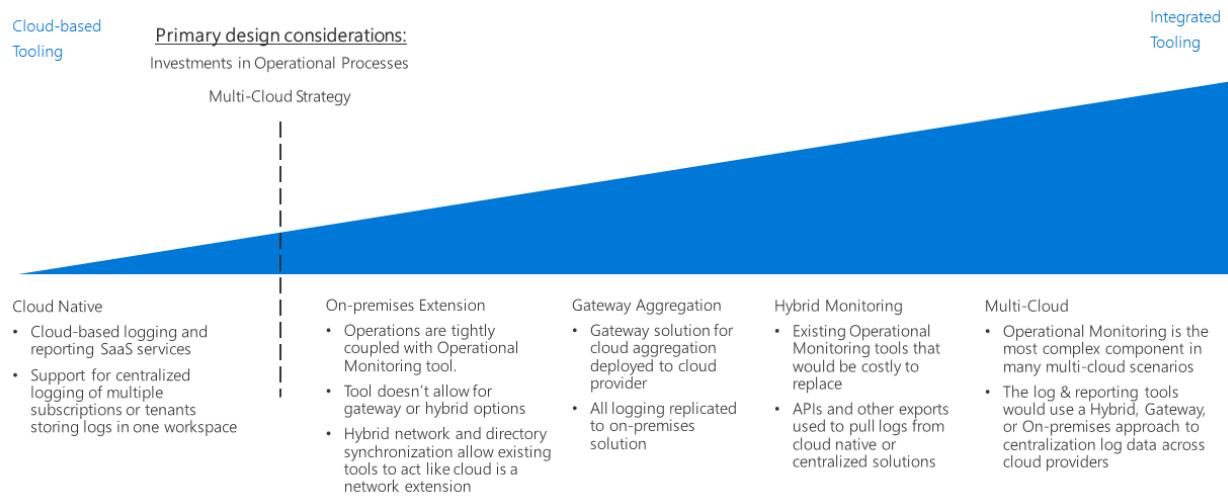
For reference architectures showing how to implement hub and spoke networks on Azure, see:

- [Implement a hub and spoke network topology in Azure](#)
- [Implement a hub and spoke network topology with shared services in Azure](#)

# Logging and reporting decision guide

11/9/2020 • 7 minutes to read • [Edit Online](#)

All organizations need mechanisms for notifying IT teams of performance, uptime, and security issues before they become serious problems. A successful monitoring strategy allows you to understand how the individual components that make up your workloads and networking infrastructure are performing. Within the context of a public cloud migration, integrating logging and reporting with any of your existing monitoring systems, while surfacing important events and metrics to the appropriate IT staff, is critical in ensuring your organization is meeting uptime, security, and policy compliance goals.



Jump to: [Planning your monitoring infrastructure](#) | [Cloud-native](#) | [On-premises extension](#) | [Gateway aggregation](#) | [Hybrid monitoring \(on-premises\)](#) | [Hybrid monitoring \(cloud-based\)](#) | [Multicloud](#) | [Learn more](#)

The inflection point when determining a cloud logging and reporting strategy is based primarily on existing investments your organization has made in operational processes, and to some degree any requirements you have to support a multicloud strategy.

Activities in the cloud can be logged and reported in multiple ways. Cloud-native and centralized logging are two common managed service options that are driven by the subscription design and the number of subscriptions.

## Plan your monitoring infrastructure

When planning your deployment, you need to consider where logging data is stored and how you will integrate cloud-based reporting and monitoring services with your existing processes and tools.

QUESTION	CLOUD-NATIVE	ON-PREMISES EXTENSION	HYBRID MONITORING	GATEWAY AGGREGATION
Do you have an existing on-premises monitoring infrastructure?	No	Yes	Yes	No
Do you have requirements preventing storage of log data on external storage locations?	No	Yes	No	No

QUESTION	CLOUD-NATIVE	ON-PREMISES EXTENSION	HYBRID MONITORING	GATEWAY AGGREGATION
Do you need to integrate cloud monitoring with on-premises systems?	No	No	Yes	No
Do you need to process or filter telemetry data before submitting it to your monitoring systems?	No	No	No	Yes

### Cloud-native

If your organization currently lacks established logging and reporting systems, or if your planned deployment does not need to be integrated with existing on-premises or other external monitoring systems, a cloud-native SaaS solution such as [Azure Monitor](#), is the simplest choice.

In this scenario, all log data is recorded and stored in the cloud, while the logging and reporting tools that process and surface information to IT staff are provided by the Azure platform and Azure Monitor.

Custom logging solutions based on Azure Monitor can be implemented as needed for each subscription or workload in smaller or experimental deployments. These solutions are organized centrally to monitor log data across your entire cloud estate.

**Cloud-native assumptions:** Using a cloud-native logging and reporting system assumes the following:

- You do not need to integrate the log data from your cloud workloads into existing on-premises systems.
- You will not be using your cloud-based reporting systems to monitor on-premises systems.

### On-premises extension

It might require substantial redevelopment effort for applications and services migrating to the cloud to use cloud-based logging and reporting solutions such as Azure Monitor. In these cases, consider allowing these workloads to continue sending telemetry data to existing on-premises systems.

To support this approach, your cloud resources must communicate directly with your on-premises systems through a combination of [hybrid networking](#) and [cloud-hosted domain services](#). With this in place, the cloud virtual network functions as a network extension of the on-premises environment. Therefore, cloud-hosted workloads can communicate directly with your on-premises logging and reporting system.

This approach capitalizes on your existing investment in monitoring tooling with limited modification to any cloud-deployed applications or services. This is often the fastest approach to support monitoring during a lift and shift migration. But it won't capture log data produced by cloud-based PaaS and SaaS resources, and it will omit any VM-related logs generated by the cloud platform itself such as VM status. As a result, this pattern should be a temporary solution until a more comprehensive hybrid monitoring solution is implemented.

On-premises-only assumptions:

- You need to maintain log data only in your on-premises environment only, either in support of technical requirements or due to regulatory or policy requirements.
- Your on-premises systems do not support hybrid logging and reporting or gateway aggregation solutions.
- Your cloud-based applications can submit telemetry directly to your on-premises logging systems or monitoring agents that submit to on-premises can be deployed to workload VMs.
- Your workloads don't depend on PaaS or SaaS services that require cloud-based logging and reporting.

### Gateway aggregation

For scenarios where the amount of cloud-based telemetry data is large or existing on-premises monitoring systems need log data modified before it can be processed, a log data [gateway aggregation](#) service might be required.

A gateway service is deployed to your cloud provider. Then, relevant applications and services are configured to submit telemetry data to the gateway instead of a default logging system. The gateway can then process the data: aggregating, combining, or otherwise formatting it before then submitting it to your monitoring service for ingestion and analysis.

Also, a gateway can be used to aggregate and preprocess telemetry data bound for cloud-native or hybrid systems.

Gateway aggregation assumptions:

- You expect large volumes of telemetry data from your cloud-based applications or services.
- You need to format or otherwise optimize telemetry data before submitting it to your monitoring systems.
- Your monitoring systems have APIs or other mechanisms available to ingest log data after processing by the gateway.

### Hybrid monitoring (on-premises)

A hybrid monitoring solution combines log data from both your on-premises and cloud resources to provide an integrated view into your IT estate's operational status.

If you have an existing investment in on-premises monitoring systems that would be difficult or costly to replace, you might need to integrate the telemetry from your cloud workloads into preexisting on-premises monitoring solutions. In a hybrid on-premises monitoring system, on-premises telemetry data continues to use the existing on-premises monitoring system. Cloud-based telemetry data is either sent to the on-premises monitoring system directly, or the data is sent to Azure Monitor then compiled and ingested into the on-premises system at regular intervals.

**On-premises hybrid monitoring assumptions:** Using an on-premises logging and reporting system for hybrid monitoring assumes the following:

- You need to use existing on-premises reporting systems to monitor cloud workloads.
- You need to maintain ownership of log data on-premises.
- Your on-premises management systems have APIs or other mechanisms available to ingest log data from cloud-based systems.

#### TIP

As part of the iterative nature of cloud migration, transitioning from distinct cloud-native and on-premises monitoring to a partial hybrid approach is likely as the integration of cloud-based resources and services into your overall IT estate matures.

### Hybrid monitoring (cloud-based)

If you do not have a compelling need to maintain an on-premises monitoring system, or you want to replace on-premises monitoring systems with a centralized cloud-based solution, you can also choose to integrate on-premises log data with Azure Monitor to provide centralized cloud-based monitoring system.

Mirroring the on-premises centered approach, in this scenario cloud-based workloads would submit telemetry direct to Azure Monitor, and on-premises applications and services would either submit telemetry directly to Azure Monitor, or aggregate that data on-premises for ingestion into Azure Monitor at regular intervals. Azure Monitor would then serve as your primary monitoring and reporting system for your entire IT estate.

**Cloud-based hybrid monitoring assumptions:** Using cloud-based logging and reporting systems for hybrid

monitoring assumes the following:

- You don't depend on existing on-premises monitoring systems.
- Your workloads do not have regulatory or policy requirements to store log data on-premises.
- Your cloud-based monitoring systems have APIs or other mechanisms available to ingest log data from on-premises applications and services.

## Multicloud

Integrating logging and reporting capabilities across a multiple-cloud platform can be complicated. Services offered between platforms are often not directly comparable, and logging and telemetry capabilities provided by these services differ as well.

Multicloud logging support often requires the use of gateway services to process log data into a common format before submitting data to a hybrid logging solution.

## Learn more

[Azure Monitor](#) is the default reporting and monitoring service for Azure. It provides:

- A unified platform for collecting application telemetry, host telemetry (such as VMs), container metrics, Azure platform metrics, and event logs.
- Visualization, queries, alerts, and analytical tools. It can provide insights into virtual machines, guest operating systems, virtual networks, and workload application events.
- [REST APIs](#) for integration with external services and automation of monitoring and alerting services.
- [Integration](#) with many popular third-party vendors.

## Next steps

Logging and reporting is just one of the core infrastructure components requiring architectural decisions during a cloud adoption process. Visit the architectural decision guides overview to learn about alternative patterns or models used when making design decisions for other types of infrastructure.

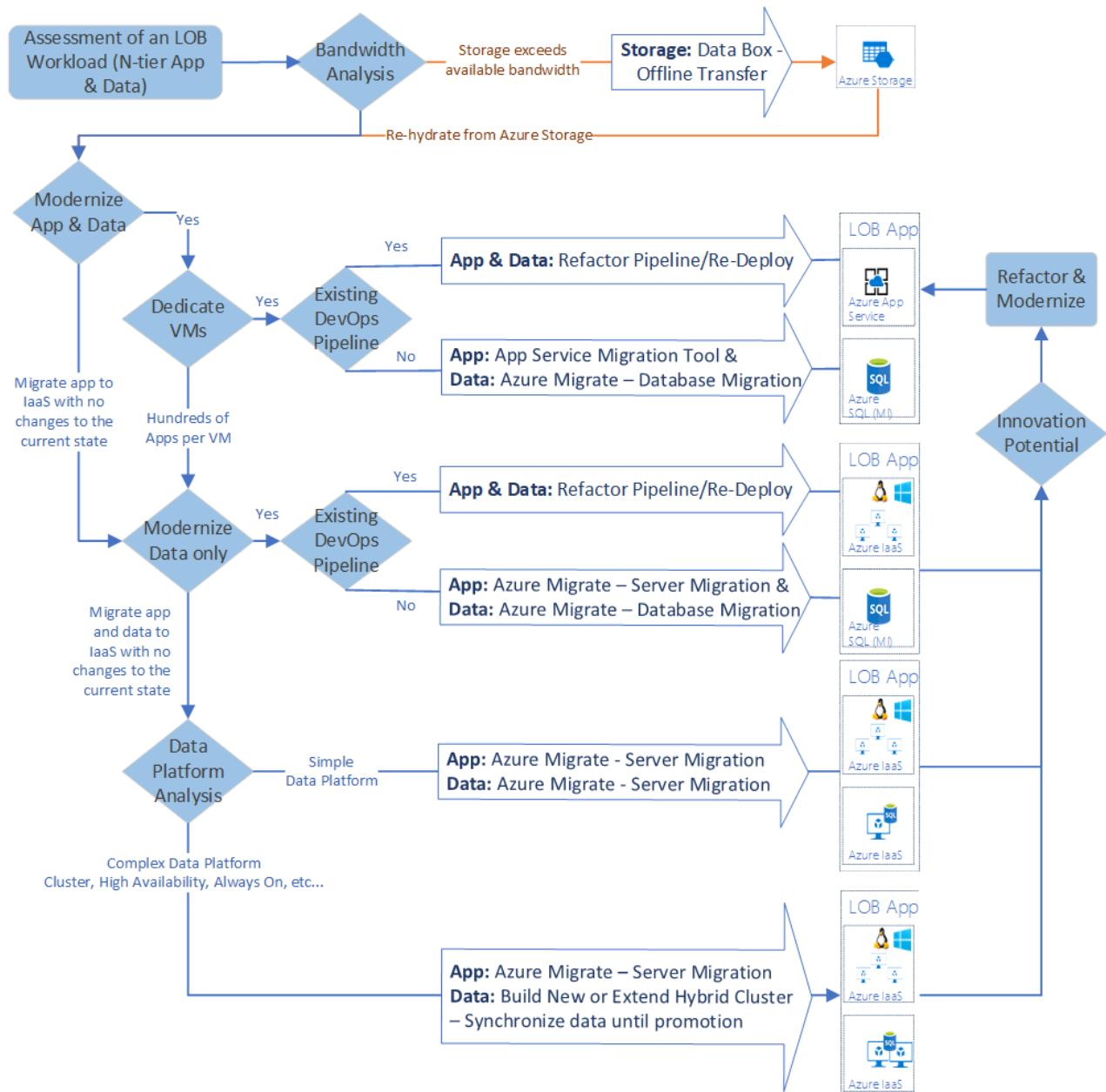
[Architectural decision guides](#)

# Migration tools decision guide

11/9/2020 • 4 minutes to read • [Edit Online](#)

The strategy and tools you use to migrate an application to Azure will largely depend on your business motivations, technology strategies, and timelines, as well as a deep understanding of the actual workload and assets (infrastructure, apps, and data) being migrated. The following decision tree serves as high-level guidance for selecting the best tools to use based on migration decisions. Treat this decision tree as a starting point.

The choice to migrate using platform as a service (PaaS) or infrastructure as a service (IaaS) technologies is driven by the balance between cost, time, existing technical debt, and long-term returns. IaaS is often the fastest path to the cloud with the least amount of required change to the workload. PaaS could require modifications to data structures or source code, but produces substantial long-term returns in the form of reduced operating costs and greater technical flexibility. In the following diagram, the term *modernize* is used to reflect a decision to modernize an asset during migration and migrate the modernized asset to a PaaS platform.



## Key questions

Answering the following questions will allow you to make decisions based on the above tree.

- **Would modernization of the application platform during migration prove to be a wise investment of time, energy, and budget?** PaaS technologies such as Azure App Service or Azure Functions can increase deployment flexibility and reduce the complexity of managing virtual machines to host applications. Applications may require refactoring before they can take advantage of these cloud-native capabilities, potentially adding significant time and cost to a migration effort. If your application can migrate to PaaS technologies with a minimum of modifications, it is likely a good candidate for modernization. If extensive refactoring would be required, a migration using IaaS-based virtual machines may be a better choice.
- **Would modernization of the data platform during migration prove to be a wise investment of time, energy, and budget?** As with application migration, Azure PaaS managed storage options, such as Azure SQL Database, Azure Cosmos DB, and Azure Storage, offer significant management and flexibility benefits, but migrating to these services may require refactoring of existing data and the applications that use that data. Data platforms typically require less refactoring than the application platform would. Therefore, it's common for the data platform to be modernized, even though the application platform remains the same. If your data can be migrated to a managed data service with minimal changes, it is a good candidate for modernization. Data that would require extensive time or cost to be refactored to use these PaaS services may be better migrated using IaaS-based virtual machines to better match existing hosting capabilities.
- **Is your application currently running on dedicated virtual machines or sharing hosting with other applications?** Application running on dedicated virtual machines may be more easily migrated to PaaS hosting options than applications running on shared servers.
- **Will your data migration exceed your network bandwidth?** Network capacity between your on-premises data sources and Azure can be a bottleneck on data migration. If the data you need to transfer faces bandwidth limitations that prevent efficient or timely migration, you may need to look into alternative or offline transfer mechanisms. The Cloud Adoption Framework's [article on migration replication](#) discusses how replication limits can affect migration efforts. As part of your migration assessment, consult your IT teams to verify your local and WAN bandwidth is capable of handling your migration requirements. Also see the [migration scenario for handling storage requirements that exceed network capacity during a migration](#).
- **Does your application make use of an existing DevOps pipeline?** In many cases, Azure Pipelines can be easily refactored to deploy applications to cloud-based hosting environments.
- **Does your data have complex data storage requirements?** Production applications usually require data storage that is highly available, offers always-on functionality and similar service uptime and continuity features. Azure PaaS-based managed database options, such as Azure SQL Database, Azure Database for MySQL, and Azure Cosmos DB all offer 99.99 percent uptime service-level agreements. Conversely, IaaS-based SQL Server on Azure VMs offers single-instance service-level agreements of 99.95 percent. If your data cannot be modernized to use PaaS storage options, guaranteeing higher IaaS uptime will involve more complex data storage scenarios such as running SQL Server Always On clusters and continuously syncing data between instances. This can involve significant hosting and maintenance costs, so balancing uptime requirements, modernization effort, and overall budgetary impact is important when considering your data migration options.

## Innovation and migration

In line with the Cloud Adoption Framework's emphasis on [incremental migration](#) efforts, an initial decision on migration strategy and tooling does not rule out future innovation efforts to update an application to take advantage of opportunities presented by the Azure platform. While an initial migration effort might focus primarily on rehosting using an IaaS approach, you should plan to revisit your cloud-hosted application portfolio regularly to investigate optimization opportunities.

## Learn more

- [Cloud fundamentals: Overview of Azure compute options](#): Provides information on the capabilities of

Azure IaaS and PaaS compute options.

- **Cloud fundamentals: Choose the right data store:** Discusses PaaS storage options available on the Azure platform.
- **Migration best practices: Data requirements exceed network capacity during a migration effort:** Discusses alternative data migration mechanisms for scenarios where data migration is hindered by available network bandwidth.
- **SQL Database: Choose the right SQL Server option in Azure:** Discussion of the options and business justifications for choosing to host your SQL Server workloads in a managed infrastructure (IaaS) or a managed service (PaaS) environment.

# Cloud Operating Model is now part of the Microsoft Cloud Adoption Framework for Azure

11/9/2020 • 2 minutes to read • [Edit Online](#)

In early 2018, Microsoft released the Cloud Operating Model (COM). The COM was a guide that helped customers understand the *what* and the *why* of digital transformation. This helped customers get a sense of all the areas that needed to be addressed: business strategy, culture strategy, and technology strategy. What was not included in the COM were the specific *how-to* steps, which left customers wondering, "Where do we go from here?"

The Microsoft Cloud Adoption Framework for Azure, is designed to help you understand the **what** and **why** and provide unified guidance on the **how** to help accelerate your cloud adoption efforts.

## Using Cloud Operating Model practices within the Cloud Adoption Framework

For an approach that's similar to the COM, begin with one of the following:

- [Get started: Accelerate migration](#)
- [Get started: Build and innovate in the cloud](#)
- [Enable success with a sound operating model](#)

# Azure enterprise scaffold is now the Microsoft Cloud Adoption Framework for Azure

11/9/2020 • 2 minutes to read • [Edit Online](#)

The Azure enterprise scaffold has been integrated into the Microsoft Cloud Adoption Framework for Azure. The goals of the enterprise scaffold are now addressed in the [Ready methodology](#) of the Cloud Adoption Framework. The enterprise scaffold content has been deprecated.

To begin using the Cloud Adoption Framework, see:

- [Ready overview](#)
- [Azure landing zones](#)
- [Landing zone considerations](#).

If you need to review the deprecated content, see the [Azure enterprise scaffold](#).

# Azure Virtual Datacenter

11/9/2020 • 2 minutes to read • [Edit Online](#)

A more robust platform architecture and implementation has been created to build on the prior Azure Virtual Datacenter (VDC) approach. [Enterprise-scale landing zones](#) in the Microsoft Cloud Adoption Framework for Azure are now the recommended approach for larger cloud-adoption efforts.

The following guidance serves as a significant part of the foundation for the [Ready methodology](#) and the [Govern methodology](#) in the Cloud Adoption Framework. To support customers making this transition, the following resources are archived and maintained in a separate GitHub repository.

- [Azure Virtual Datacenter](#): This eBook shows you how to deploy enterprise workloads to the Azure cloud platform while respecting your existing security and networking policies.
- [Azure Virtual Datacenter lift-and-shift guide](#): This white paper discusses the process that enterprise IT staff and decision makers can use to identify and plan the migration of applications and servers to Azure using a lift-and-shift approach while minimizing any additional development costs and optimizing cloud hosting options.