

Microsoft Azure Cloud Adoption Framework Server Migration

(Windows, Linux, VMWare)

Disclaimer

© 2020 Microsoft Corporation. All rights reserved. This document is provided "as-is." Information and views expressed in this document, including URL and other Internet Web site references, may change without notice.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. Microsoft customers and partners may copy, use and share these materials for planning, deployment and adoption of Microsoft Cloud Adoption Methodology.

**MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.**

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation. Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, our provision of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property. The descriptions of other companies’ products in this document, if any, are provided only as a convenience to you. Any such references should not be considered an endorsement or support by Microsoft. Microsoft cannot guarantee their accuracy, and the products may change over time. Also, the descriptions are intended as brief highlights to aid understanding, rather than as thorough coverage. For authoritative descriptions of these products, please consult their respective manufacturers. © 2019 Microsoft Corporation. All rights reserved. Any use or distribution of these materials without express authorization of Microsoft Corp. is strictly prohibited. Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

**We look forward to your feedback!**

Thank you for your continued trust and partnership. The resources within this toolkit will be iteratively improved upon based on product releases as well as direct feedback from delivered engagements. We encourage you to provide feedback to help us improve our products and toolkits. Please use the feedback process available through following web site: <http://aka.ms/cafenablementkit>

TABLE OF Contents

[1 Introduction 1](#_Toc42628510)

[2 Document purpose 1](#_Toc42628511)

[3 Audience 1](#_Toc42628512)

[4 Define Strategy 2](#_Toc42628513)

[4.1 Define Strategy CAF Plan Template 4](#_Toc42628514)

[5 Plan 6](#_Toc42628515)

[5.1 Inventory and Rationalize Digital Estate 8](#_Toc42628516)

[5.1.1 Cloud Assessment 8](#_Toc42628517)

[5.2 Organizational alignment to support the Adaption plan 11](#_Toc42628518)

[5.3 Skills Readiness and Role Based Responsibilities 11](#_Toc42628519)

[5.4 Develop Cloud Adoption plan 12](#_Toc42628520)

[6 Ready 13](#_Toc42628521)

[6.1 Azure Setup and Configuration 13](#_Toc42628522)

[6.1.1 Azure Cloud Resources 14](#_Toc42628523)

[6.1.2 Azure Role Based Access 15](#_Toc42628524)

[6.1.3 Cost and Billing of Azure resources 19](#_Toc42628525)

[7 Adopt (Migrate) 22](#_Toc42628526)

[7.1 Migration Overview 22](#_Toc42628527)

[7.2 Migration Strategy 23](#_Toc42628528)

[7.3 Migration: Deployment 23](#_Toc42628529)

[8 Govern 23](#_Toc42628530)

[8.1 Governance, Security and Compliance 28](#_Toc42628531)

[9 Manage 34](#_Toc42628532)

[9.1 Inventory and visibility 35](#_Toc42628533)

[9.2 Operational compliance 36](#_Toc42628534)

[9.3 Protect and recover 36](#_Toc42628535)

[9.4 Monitoring and Reporting 36](#_Toc42628536)

[Appendix A - References 39](#_Toc42628537)

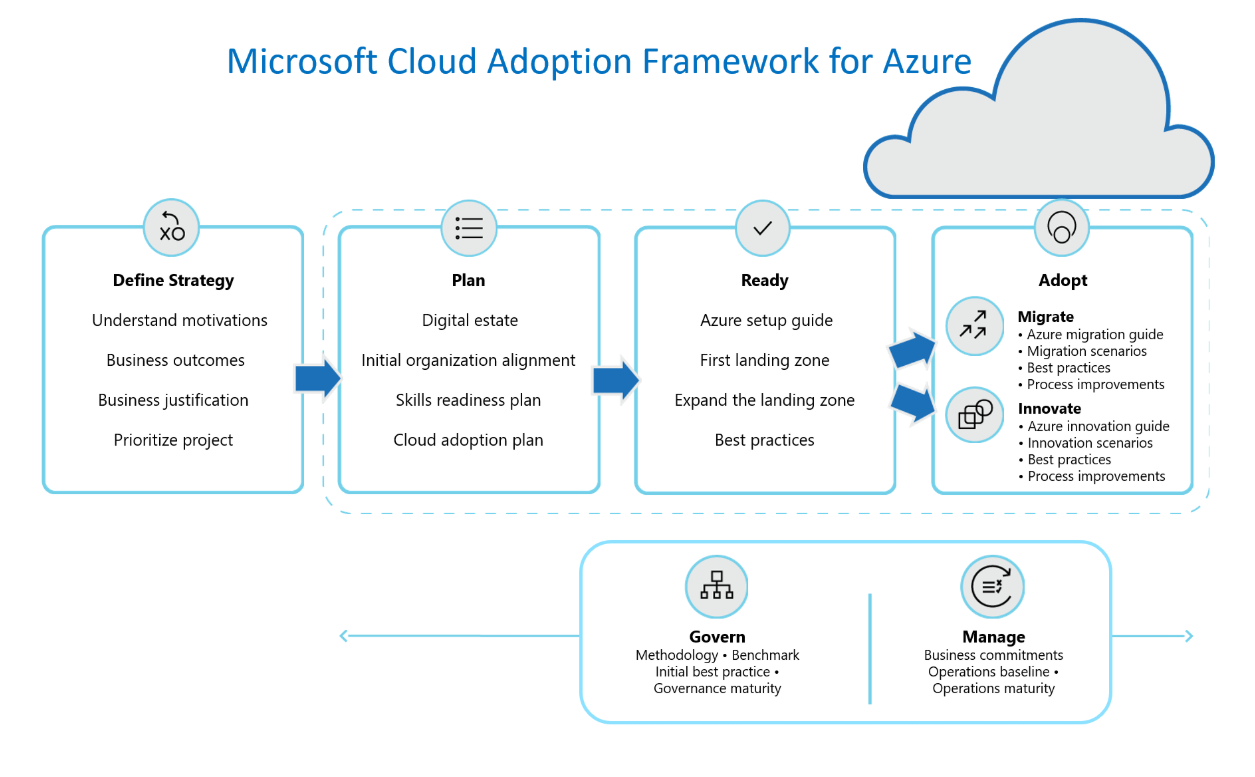
[Appendix B: Documentation Revision Table 40](#_Toc42628538)

# Introduction

[Microsoft Cloud adoption framework for Azure](https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/strategy/cloud-migration-business-case) (CAF) is a very powerful cloud adoption methodology.

The primary goal of this document is to provide partners (and customers) a design reference in line with CAF which they can leverage to build and deploy server workload migration to cloud.

Find below Cloud adoption framework for ready reference which can help you define and execute server migration to Azure.



# Document purpose

Lift & Shift is one of many migration approaches and this guide specifically covers fast track Cloud Adoption approach using rehost (lift and shift) Cloud Adoption Strategy for Microsoft Windows, Linux, Hyper V and VMWare type of workloads.

# Audience

This document is primarily intended to be used by partners to enable customer for efficient and Cloud Adaption Framework aligned, design and execution of Server Migration that includes Physical Servers, Virtual Servers like Hyper-V VMs and VMWare VMs.

# Define Strategy

Define strategy is the first pillar of the successful cloud adoption and mostly remain rigid once defined except for few minor changes. Overall strategy is defined at the start of cloud engagement based on numerous factors influencing decisions like motivations, Business Outcome, and justification.

Cloud strategy development is an evolutionary process in most enterprises. It requires coordination among a variety of stakeholders including Management, Business, IT professionals, developers, compliance experts, procurement, and security.

Successful strategy is an outcome and one of the effective ways to define strategy is to adopt best practices for planning and running strategy discussions. Business strategy goes hand in hand with technology strategy and people strategy.

4 Steps process for the Cloud Adoption Strategy follows,

1. Motivations:

Meet the key stakeholders and executives to document the motivations behind cloud adaption

1. Business Outcomes:

Engage motivated stakeholders and executives to document specific business outcomes,

1. Business Justification:

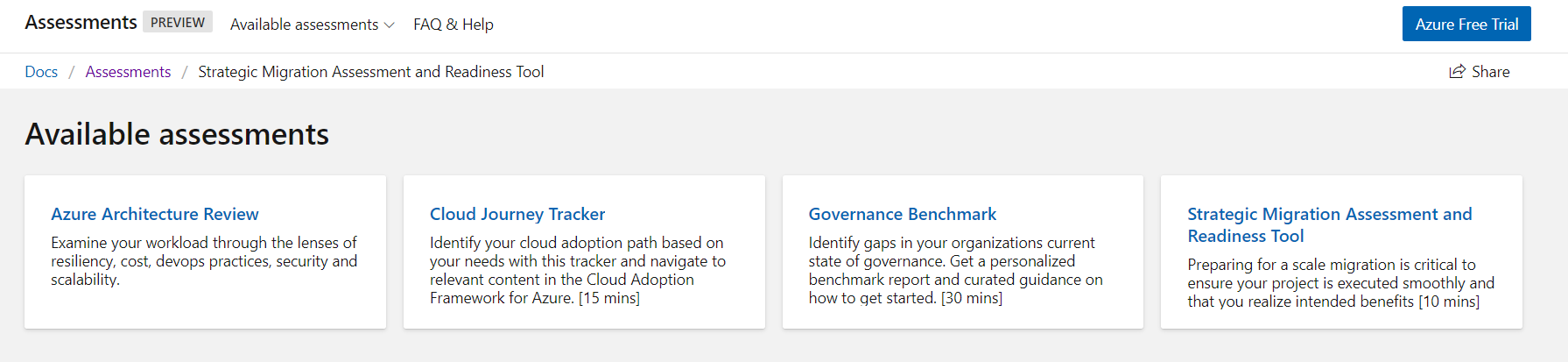
Develop a business case to validate the financial model that supports your motivations and outcomes.

1. Choose the right first project:

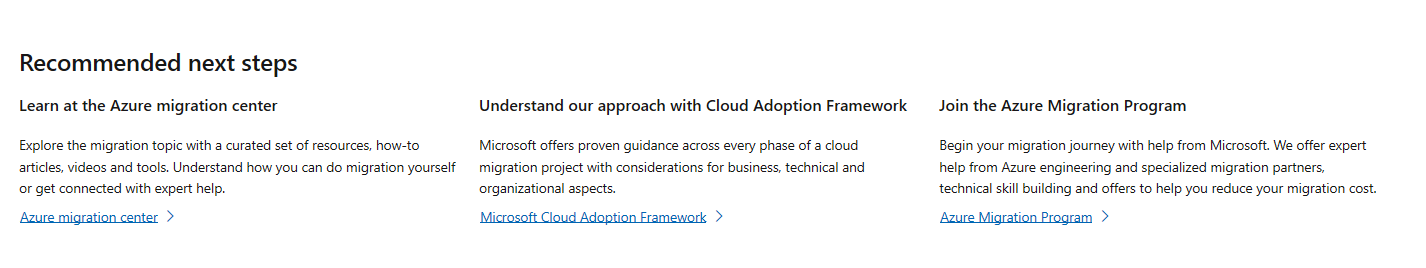
Your first cloud adaption project will help align motivations with technical effort.

If not already defined and documented start with defining strategy using below best practices.

* Start with defining Cloud center of excellence for the strategy discussions.
* Stakeholders aware of relevant resources like [motivations](https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/strategy/motivations) , [business outcome](https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/strategy/business-outcomes/), [business justification](https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/strategy/cloud-migration-business-case), other [resources and skill](https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/strategy/suggested-skills) and [Microsoft Cloud Adoption Plan template](https://archcenter.blob.core.windows.net/cdn/fusion/readiness/Microsoft-Cloud-Adoption-Framework-Strategy-and-Plan-Template.docx). Also, it is more important to know what CAF is not and cloud strategy is ongoing journey which need to be refined periodically based on major business events.
* Relevant participants can visit [Microsoft Assessments](https://docs.microsoft.com/en-us/assessments/) . This is a set of tools where Customers can evaluate their business strategies and receive curated guidance from Microsoft Assessments. Specifically Cloud Journey Tracker – Helps with cloud adoption path based on your needs and navigate to relevant content in the Cloud Adoption Framework for Azure and Strategic Migration Assessment and Readiness Tool



[Strategic Migration Assessment and Readiness Tool](https://docs.microsoft.com/en-us/assessments/). prepare for a migration and is critical to ensure your project is executed smoothly and that you realize intended benefits



**Business Strategy**

Motivations to Business transformation that are supported by cloud adaption can be driven by various motivations.

Recommendation that cloud adoption team 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 |

During actual discussion team can brainstorm and discuss various topics and priorities related to cloud adoption. Stakeholders might already know business issues, financial issues, and a broad range of technology issues they face. Some questions to ask include:

* What do you expect from your move to the cloud?
* What are you moving to the cloud today?
* How has your transition to the cloud changed your organization?
* What is our short-term and long-term roadmap for moving to the cloud??
* How are you thinking about dual cloud?
* What are the criteria which define where apps or data reside?
* What are the risks which you have identified?
* What are the next applications and databases which you have identified to move to the cloud?
* What benefits (i.e. agility, cost savings, scalability, etc.) are we expecting from the cloud and how do we prioritize them?
* What is my personal roadmap for building the necessary cloud skills?
* How can we continue to derive the maximum benefit from existing investments?
* How do we want to design future solutions to best leverage the cloud?

## Define Strategy CAF Plan Template

Once finalized cloud adoption priorities stake ranked and details can be captured in the [Microsoft Cloud Adoption Plan template](https://archcenter.blob.core.windows.net/cdn/fusion/readiness/Microsoft-Cloud-Adoption-Framework-Strategy-and-Plan-Template.docx).

**Motivations and drivers**

Why do you want to adopt the cloud? Are there critical business events driving your decision? Do you have specific business [motivations](https://docs.microsoft.com/azure/architecture/cloud-adoption/business-strategy/motivations-why-are-we-moving-to-the-cloud)?

[Understand and describe business situation, implications and details on business events driving the move to the cloud]

**Business outcomes**

What are the expected [business outcomes](https://docs.microsoft.com/azure/architecture/cloud-adoption/business-strategy/business-outcomes/) from adopting the cloud? Collect them in the corresponding table below, organized by priority.

*High Priority*

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Stakeholder: |  | |  | Outcome: |  | |
|  |  |  |  |  |  |  |
| Business Drivers | | |  | KPI |  | Capabilities |
| List any business drivers | | |  | List success metrics |  | List necessary capabilities |

*Mid Priority*

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Stakeholder: |  | |  | Outcome: |  | |
|  |  |  |  |  |  |  |
| Business Drivers | | |  | KPI |  | Capabilities |
| List any business drivers | | |  | List success metrics |  | List necessary capabilities |

*Low Priority*

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Stakeholder: |  | |  | Outcome: |  | |
|  |  |  |  |  |  |  |
| Business Drivers | | |  | KPI |  | Capabilities |
| List any business drivers | | |  | List success metrics |  | List necessary capabilities |

**Business justification**

How would you measure success? Beyond achieving the business outcomes, are there other indicators for successful Azure adoption in your organization?

Consider creating a business case for adopting Azure and create a [financial model](https://docs.microsoft.com/azure/architecture/cloud-adoption/business-strategy/financial-models) to support this plan.

As part of strategy of moving to the cloud is understanding the technology, but you also have to consider business and organizational impacts. Typical stages organizations go through include:

* Cloud aware - IT staff is aware of broad cloud trends
* Cloud experimentation - IT organization begins to learn about various cloud services such as Software as a Service, Platform as a Service, and Infrastructure as a Service
* Opportunistic cloud - IT organization begins to actively migrate workloads to cloud to meet new business requirements
* Cloud first - Default assumption is that cloud services will fulfill the majority of the computing needs

Migrate Rehost (lift and shift) scenario loosely fall under Opportunistic cloud phase and it is assumed that relevant strategy already defined and specific motivations, business outcome and justifications captured. Find below few of the captured strategy details in-line with the current migrate Rehost scenario.

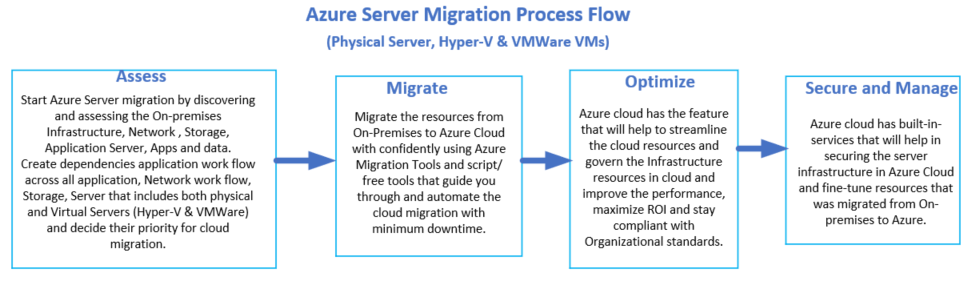
* Address business growth
* Increase efficiency
* Increase agility
* Cloud Scale
* Limit risk
* Assure business continuity and data protection
* Extend (Hybrid Cloud
* Data Center Migration
* Return On investments
* Cost Saving
* Compliance
* Security
  + Additionally, Azure Security Center helps you:
    - Understand security state across workloads. Manage security on-premises, Azure, and other cloud platforms—in one console. Built-in dashboards provide instant insights into potential security issues.
    - Extend advanced threat protection to your workloads. Continuously monitor the security of your machines, and networks across hybrid environments using hundreds of built-in security assessments.

# Plan

Microsoft Azure provides extensive tooling to assess, plan and execute a migration to the cloud.

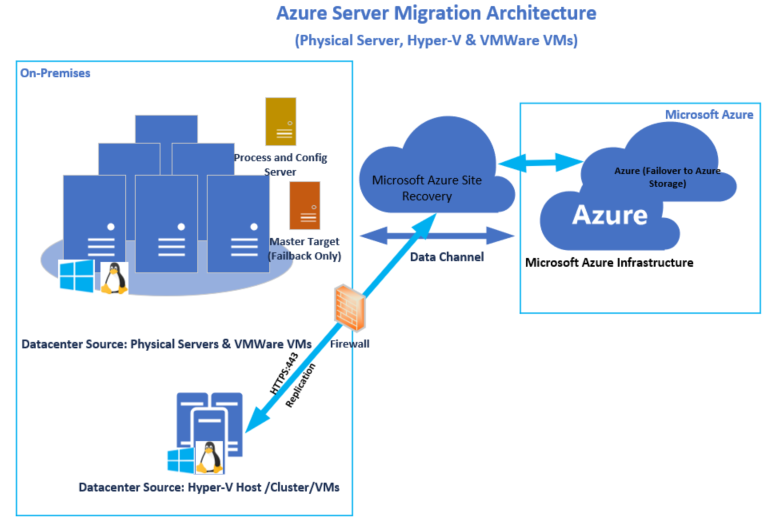
In this section we are going to build a cloud adaption plan considering the business goals and make any changes across digital estate, skills, and organization. The total cost of ownership (TCO) of the company’s entire Infrastructure environment portfolio will be assessed, identifying key patterns and select correct migration treatment for each server and network based on TCO report and Infrastructure requirement.

**Server Migration Process workflow**



In the assessment stage, you map out on-premises applications, servers, storage and endpoints, their dependencies and configuration, and plan the sizing and cost of the projected Azure deployment.

Key Considerations for the assessment stage:

1. Networking: Creating Virtual network to maintain good performance and stability that was available in on-premises datacenter.
2. Storage: Based on On-premises storage assessment, review the Azure storage services and select a solution that allowed number of operations per second and the purpose of the data as hot vs cold.
3. Scalability: Cost modeling is required for configuring the Azure auto scale option and dynamic scaling of application can be selected.

Cloud Adaption Planning includes the below main process,

* Inventory and rationalize digital estate
* Organizational alignment to support the Adaption plan
* Skills Readiness and Role based Responsibilities
* Develop cloud adaption plan for above areas

## Inventory and Rationalize Digital Estate

Every company has a digital estate in our case it is physical servers, virtual machines, application servers, network, storage, security which plays direct role in powering businesses and supporting business operation.

Planning a digital estate is the most obvious first step while you are migrating your digital estate to the cloud. Below Steps is considered as best way to plan digital estate starting with the analysis approach, gathering inventory data, rationalize the digital estate and finally building cost models.

### Cloud Assessment

The Cloud assessment provides a holistic view of the physical and virtual computing environment from a hardware, storage, network, and compute perspective.

To leverages the available asset inventory data provided by Networks Cloudscape, Microsoft Active Directory, Microsoft System Center Configuration Manager (SCCM), the Service Now CMDB, and various Virtualization tools in the organization. The combination of these data sources allows for a base analysis of the infrastructure and workload running in domains. The resulting combined data provides an analytical path to compatibility of hardware, storage, network, compute, and software, helping to determine an estimated cost and effective plan for deployment of Microsoft Azure.

The Cloud Assessment report is broken down in four sections to provide a comprehensive analysis to provide environment assessment, Cost modeling, technical compatibility, and migration approaches. The sections are labeled Environment Assessment, Infrastructure Assessment, Technical Assessment, and Migration Assessment.

Table 1.0 Azure Assessments Overview

|  |  |
| --- | --- |
| Section | Description |
| Environment Assessment | Provides a holistic discovery and high-level analysis of the scope of the environment, criteria, and Azure pricing used for this assessment. |
| Infrastructure Assessment(s) | **Inventory Assessment Model**  This assessment is a like-to-like mapping of the virtualized and non-virtualized system configurations to an equivalent Azure instance and storage size. This mapping is based on system hardware specifications (e.g. number of CPUs, CPU speed, and assigned memory, disk size, etc.). This mapping does not take actual workload or usage into account. Total Cost of Ownership (TCO) is estimated based on this configuration.  **Right-Sized Assessment Model**  This assessment considers virtualized and non-virtualized system configurations and incorporates actual workload performance usage characteristics as provided from the different management tools. That data is then projected to an Azure environment. Mapping of instance sizes, storage, and network demand is provided and the TCO is estimated based on the suggested configuration. |
| Technical Assessment(s) | **Infrastructure Compatibility Assessment**  This assessment analyzes existing operating systems, server roles / features, and enterprise application groupings and determines the most likely compatibility in an Azure environment per the current information available.  **Application Assessment**  This assessment helps to understand the Application to Server rationalization process and how to use this data in conjunction with the infrastructure and compatibility assessments to build a migration criteria and plan.  **Cloud Services Assessment**  This Cloud Assessment provides a base set of technical requirements for products and features required in Azure. The assessment was provided by technical workshops performed during the engagement to determine the Azure features required for use, based on technology strategy and requirements for migrating, running, and reporting on systems in a cloud environment. |
| Migration Assessments | **Migration Process**  This assessment helps to understand the full scope of a migration for the specific Client, each client has diverse needs and IT models that will dictate the overarching migration process and help to understand the costs associated with the required migration process.  **Migration Resources**  This assessment helps to understand the combined resourcing model.  **Migration Costs**  This assessment builds upon all of the assessments to help understand both Azure subscription costs, migration project labor costs, and internal resource requirements to initiate a successful cloud migration project.  **Migration Example**  The migration Cost example leverage all the data and assessments in the workbook to build a total cost of Cloud migration. |
| BCDR Assessment | **BCDR Process**  This assessment helps to understand the full scope of a BCDR for the specific Client, each client has diverse needs and IT models that will dictate the overarching process and help to understand the costs associated with the required process.  **BCDR Resources**  This assessment helps to understand the combined resourcing model.  **BCDR Costs**  This assessment builds upon all the assessments to help understand both Azure subscription costs, BCDR project labor costs, and internal resource requirements to initiate a successful cloud DRaaS project.  **BCDR Example**  The BCDR Cost example leverages all the data and assessments in the workbook to build a total cost of Cloud protected machines. |

Figure 1.0 - Microsoft Azure Assessment Path

Microsoft Azure Assessment Path – Steps taken to assess Microsoft Azure readiness

## Organizational alignment to support the Adaption plan

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:

## Skills Readiness and Role Based Responsibilities

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.

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.

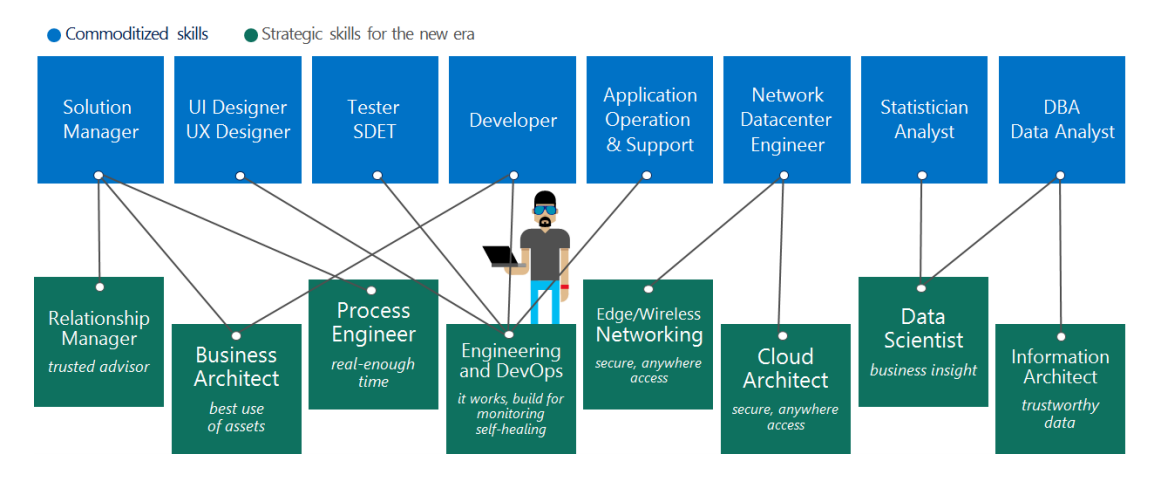


Figure 1 - Mapping of skills to IT roles in a cloud-hosted environment.

The Cloud Adoption Framework guides readers through the full adoption lifecycle. Throughout this framework, readers are provided opportunities to build necessary skills. Each of 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. Details information on the Skill readiness and role based responsibilities available in the below link, [CAF Server Migration Suggested Skills](https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/plan/suggested-skills)

## Develop Cloud Adoption plan

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](https://wikipedia.org/wiki/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.

Steps 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.

# Ready

This section covers the readiness of the cloud environment before we adopt CAF. Based on the planning prepared in the previous section we will be creating landing zone to host the infrastructure in the cloud.

Below are the major areas that we will be setting up in the cloud,

1. Azure Setup Guide
2. Cloud Infrastructure Baseline
3. Cost Analysis and Utilization of Cloud Infrastructure
4. Apply Best Practice and Configure Cloud Infrastructure

## Azure Setup and Configuration

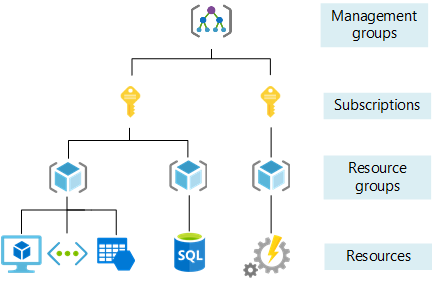
Before we adopt CAF, we must prepare the Azure Cloud environment based on the planning and current infrastructure inventory assessment.

Below is the major areas that will help to Adopt CAF and organize resources, plan and control the cost involved before and after migration, secure the infrastructure and manager the organization after the migration to cloud.

1. Organize Azure Cloud resources
2. Mange and secure access to Cloud
3. Cost and Billing of Azure Resources in Cloud
4. Plan for governance, security, and compliance
5. Use monitoring and reporting
6. Improve change management process by knowing all new features.

### Azure Cloud Resources

Azure Cloud provides four levels of management scope, that covers all the areas that required to manage the Cloud Environment. Below is the details diagram



First step before migration should be creating a management group hierarchy to simplify the management of your resources (Azure Active Directory, Virtual machines, Application Servers, Applications)

* **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.
* **Resource groups:** we must create a logical container into which Azure resources like databases, and storage accounts are deployed and managed.
* **Resources:** Resources are instances of services that you create, like virtual machines, storage, or SQL databases.

#### Azure Subscription target

Here are the Azure subscriptions targeted

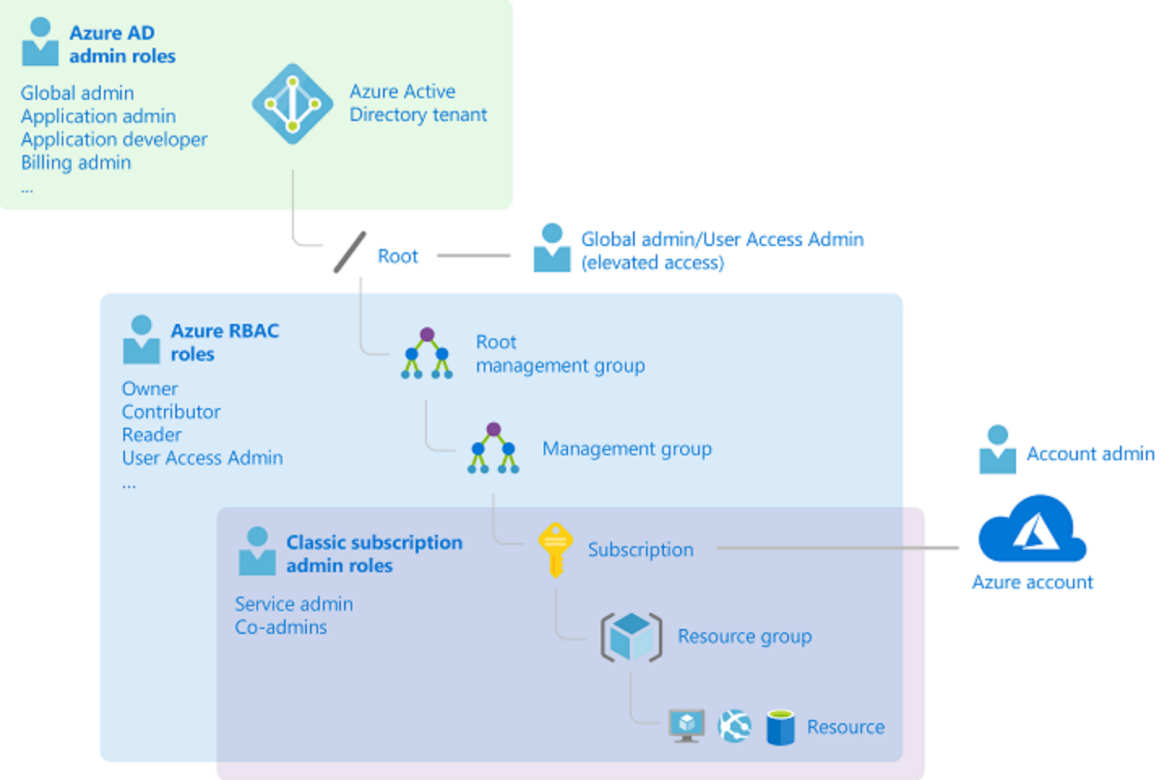
Table 4 Azure Subscription targeted

| # | Subscription Name | Type | Provisioned Y|N | ID |
| --- | --- | --- | --- | --- |
|  | <Microsoft Azure> | Production |  | ########-####-####-####-############ |
|  | <Microsoft Azure Dev\Test> | Dev\Test |  | ########-####-####-####-############ |

### Azure Role Based Access

If you are new to Azure, you may find it a little challenging to understand all the different roles in Azure. This article helps explain the following roles and when you would use each:

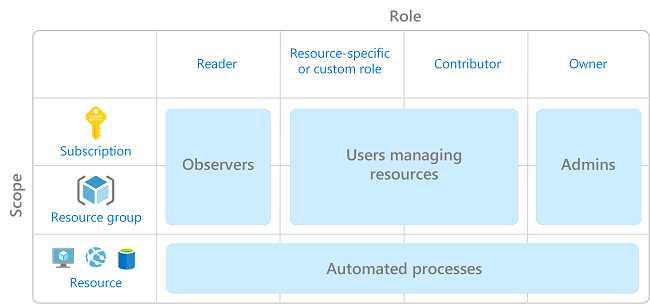
* Classic subscription administrator roles
* Azure role-based access control (RBAC) roles
* Azure Active Directory (Azure AD) administrator roles

The following diagram is a high-level view of how the classic subscription administrator roles, Azure RBAC roles, and Azure AD administrator roles are related.

#### Managing Access

The next step in the process is to Manage 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.

Below diagram will help us to build Role Based Access Control



* 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.

#### Azure tools and Approaches

Before migration we need to make sure that our source environment is supported and addressed all the possible migration option.

Source Environment (On-premises server) supported:

* Windows Servers
* Hyper V
* VMWare
* Linux

Use Azure tools to assess applications for migration and get automated recommendations regarding CPU, disk size and storage requirements, current network architecture and capacity, performance requirements, high availability and resiliency recommendations, and requirements for ongoing maintenance.

Virtual Machine Readiness Assessment tool—automatically inspects physical or virtualized assets and provides a checklist for moving them to the cloud. It provides a report saying which workloads can be moved and which require further investigation.

Microsoft Assessment and Planning (MAP) toolkit—an inventory, assessment and reporting tool that can help you plan migrations for Windows 8.1, Office 2013, Office 365, Windows Server 2012/ 2016/2019, SQL Server 2014/2019, Hyper-V, Microsoft Private Cloud Fast Track, and more environments. The MAP Toolkit assesses environments and provides readiness information for both physical and virtualized workloads migrating to Azure.

Azure Migrate is a Microsoft service that helps organizations assess the way their on-premises workloads will perform, and how much they will cost to host, in the Azure public cloud. It provides a single console to start, run, and track migrations.

Azure Migrate can check up to 35,000 VMware VMs and 10,000 Hyper-V VMs in each job, assess migration preparation, and provide actionable advice to help you save costs.

For VMware, it provides agent-based and agentless options, and for Hyper-V, it is agentless by default. It can also help you test your migration in an isolated Azure-like environment.

Azure Migrate can help you migrate the following types of workloads:

* Servers—assess and migrate on-premises servers into Azure VMs.
* Databases—check and migrate on-premises databases to Azure SQL DB, or to Azure SQL Managed Instance.
* Web applications—assess and migrate on-premises web applications to Azure App Service.
* Virtual desktops—evaluate and migrate [digital desktop infrastructure (VDI)](https://cloud.netapp.com/blog/vdi-cloud-volumes-ontap) to Azure Windows Virtual Desktop.
* Data—migrate data to Azure quickly and cost-effectively, using Azure Data Box products.
* Azure Migrate provides the following integrated tools:
* Azure Migrate: Server Assessment—discover and assess VMware VMs, Hyper-V VMs, and physical servers, to see if they are ready for migration.
* Azure Migrate: Server Migration—migrate VMware VMs, Hyper-V VMs, physical servers, and public cloud VMs to Azure.
* Web App Migration Assistant—asses on-premises websites and their infrastructure for migration to Azure App Service.
* Microsoft Movere—a SaaS platform, acquired by Microsoft and integrated into Azure, which can accurately visualize entire IT environments. It is available through the Microsoft Solution Assessment and Cloud Economics Programs.

#### Azure Migration Readiness

The following sections outline the installation process for imaging computers in a standardized manner.

#### Site-to-Site Connectivity Summary

Microsoft Azure will have two sites, which will have Active/Active gateways between Azure and Enterprise network.

The Active/Active Connection will be leveraging BGP routing to enable resiliency between the connections and the core network at the Enterprise.

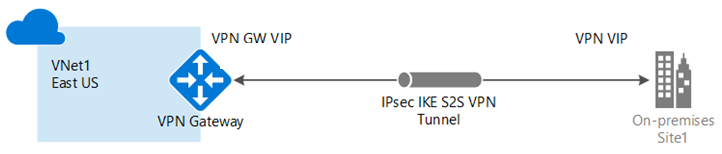
**Note:** The BGP addresses that are advertised from the Enterprise (customer premise) should suppress the advertisement of the default route address 0.0.0.0/0, unless it is a policy requirement. There are many services in Azure that are going to leverage the default route, for example Azure Storage.

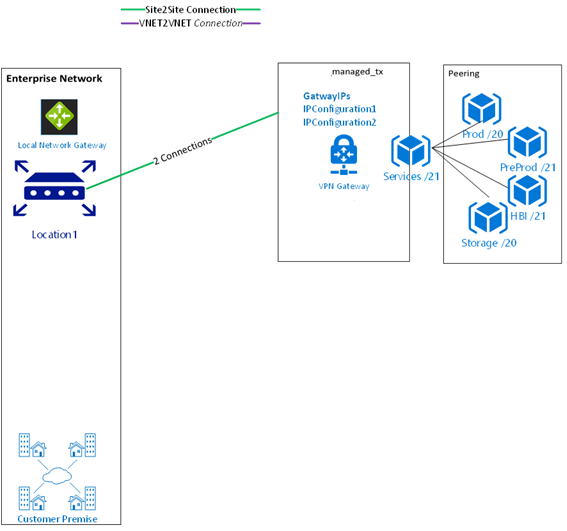
**Site-to-Site Connectivity Details**

Azure will have two Local Network Gateway for two of the connections that will define the IP address, ASN Number and BGP address of the VPN connections. The goal of the gateway is to have redundancy by having BGP routing the ability.

**VPN Creation Process**

A Site-to-Site VPN gateway connection is used to connect your on-premises network to an Azure virtual network over an IPsec/IKE (IKEv1 or IKEv2) VPN tunnel. This type of connection requires a VPN device located on-premises that has an externally facing public IP address assigned to it.





### Cost and Billing of Azure resources

**Manage your costs with Azure Cost Management**

Azure Cost Management 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.

**Cloud Environment Cost Summary**

The Cloud Cost Summary provides multiple cost models to consider when sizing your Cloud Infrastructure requirements. The inventory model and right-sized performance model provide two different perspectives for analyzing the virtual machines. The inventory model is based on a like for like hardware/virtual profile mapping to a Cloud, where the performance mapping layers on actual performance utilization and the required capacity of the machines. The major differences in the models is cost comparison on sizing the machines appropriately.

The summarized data in the section was taken from an extensive analysis in Excel that models all the virtual machines in detail to provide different cost models based on forensic data. The spreadsheets can be viewed in conjunction to provide additional context and details.

Total cost of Ownership (TCO) based on the inventory refer the cost estimation link [TOC Azure Calculator](https://azure.microsoft.com/en-us/pricing/tco/calculator/)

The following are pricing characteristics:

Table 2.0 Licensing Types Compared

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| License\Cost Type | Platform | Basis | Lowest Cost | Discount Level |
| Retail | Azure | Utilization | Azure | 0% Applied |

The following scenarios were modeled for price on Azure:

**Table 3.0 Cloud / Azure Cost Scenarios**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Scenario | Platform | Basis | Lowest Cost | Discount Level |
| 200 Applications & Infrastructure | Azure | Utilization | Azure | 35% Applied |
| All Virtual Machines | Azure | Inventory | Azure | 35% Applied |

**Inventory Cost Model Summary**

The cost model summary provides a synapsis of the costs on Azure for the applications representing the virtual machines. Only one model or hybrid would actual be used so the costs are not aggregated. All Costs have been rounded to the nearest dollar throughout the tables.

The calculations were positioned around Central US as well as West and East US pricing with the following details:

* **Target Details:** 
  + Target Location
  + Pricing tier (Standard)
  + Storage type (Premium managed disks)
  + Reserved instances (3 years reserved)
* **Sizing:**
  + Sizing criterion (As on-premises)
  + Performance history (1 Day)
  + Percentile utilization (95th)
  + VM series (6 selected)
  + Comfort factor (1.3x)
* **Pricing:**
  + Pricing Offer (Pay-As-You-Go)
  + Currency (US Dollar ($))
  + Discount (0%)
  + VM uptime (31 Days per month) x (24 Hours per day)
  + Azure Hybrid Benefit - save up to 40% with a license you already own (Yes)

**Environment Cost Model Summary**

The cost model summary provides a synapsis of the costs on Azure for all virtual machines in scope for this engagement. Only one model or hybrid would actual be used so the costs are not aggregated.

**Table 5.0 All Virtual machines Cost Model Summary**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| Model | Environment | VM Count | Cost Year | Cost Month | Cost Per VM Year | Cost Per VM Month |
|  | | | | | | |
| Inventory | All in scope  AD Server /Terminal Server Licensing / Misc./Exchange/Exchange Witness Server/ Quorum Web Server/ Quorum SQL Server | Each VM cost associate in Assessments | Each VM cost associate in Assessments | Each VM cost associate in Assessments | Each VM cost associate in Assessments | Each VM cost associate in Assessments |

**Inventory Cost Models**

The Inventory Cost Model takes the exact existing hardware profile and maps it to the lowest cost matching Cloud virtual machine. The costs are provided below for each major component in the Cloud, and rolled up for the entire datacenter environment. In addition, the percentage of free overhead capacity is shown once the infrastructure is mapped in Azure for each specific hardware component across the enterprise of machines.

The analysis was broken down into two different categories to be able to identify the best target systems to do further analysis and planning from. The breakout is as follows:

* **Rehost (Migrate)** – All Virtual Machines with Disk > 1TB, this represents all Virtual Machines that have a Non-Primary Disk drive less than 1TB.
* **Remain -** All Virtual Machines with Disk > 1TB, this represents all Virtual Machines that have a Non-Primary Disk drive greater than 1TB.

In addition, the right-sized cost model allows us to do some additional modeling using the advanced datasets from the Virtual Machines. The following fields are provided as follows for the cost model:

**Table 6.0 Field Listing**

|  |  |  |
| --- | --- | --- |
| Field Name | Data Source | Definition |
| Azure Compute Price/Year | Calculated | Price/Year \* Customer Discount |
| Azure Storage Price/Year | Calculated | Hybrid Storage Price/Month \* Customer Discount |
| Azure VM + Hybrid Storage Price/Year | Calculated | Azure Compute Price/Year + Azure Storage Price/Year |
| Azure Storage Savings/Year | Calculated | Non- Premium Storage Savings/Year \* Customer Discount |
| Azure Running % | Calculated | Estimated Workload Azure Compute Running Time |
| Azure Running Price/Year | Calculated | Azure Compute Price/Year \* Azure Running % |
| Azure VM + Storage Running Cost/Year | Calculated | Azure Running Price/Year + Azure Storage Price/Year |

Predict and manage costs

1. Go to [Cost Management + Billing](https://portal.azure.com/#blade/Microsoft_Azure_Billing/ModernBillingMenuBlade/Overview).
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](https://portal.azure.com/#blade/Microsoft_Azure_Billing/ModernBillingMenuBlade/Overview).
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](https://portal.azure.com/#blade/Microsoft_Azure_Support/HelpAndSupportBlade/overview).
2. Select **New support request**.

View a support request

To view your support requests and their status:

1. Go to [Help + Support](https://portal.azure.com/#blade/Microsoft_Azure_Support/HelpAndSupportBlade/overview).
2. Select **All support requests**.

# Adopt (Migrate)

Before you begin migrating your Physical & Virtual Servers to the Azure, you should be able to make the following assumptions:

From the Plan, Ready, and Adopt methodologies, the source data should have been identified and separated into workloads which are manageable to migrate through iterations.

## Migration Overview

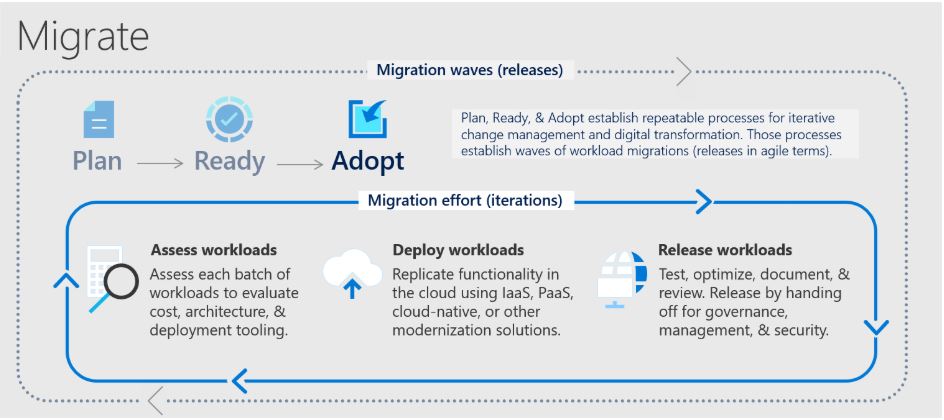
During each iteration of migrating a workload, there are 3 phases which are necessary to maximize performance.

**Assessment**: Make concrete decisions regarding cost, modernization options, and deployment tools. You should reassure that any assumptions made during the discovery phase on the data characteristics holds to be true; as well as build on top of those decisions to give the most redefined description about that data.

**Deploy workloads**: Replicate or improve performance from the source by taking advantage of tools available in the cloud such as:

* Azure Database Migration Services
* Azure Data Migration Assistant

**Release**: Once the data workloads has been deployed in the cloud, you should test, optimize, and review the newly deployed workload to ensure the correct data and functionality has been deployed.



## Migration Strategy

Four major migration strategies defined below section, based on the strategies identify the tools and technologies that will help to migrate each server, network, storage and virtual servers.

1. Do you need to leverage Azure’s hybrid cloud solutions?
2. Do you want to run in traditional VMs in containers or using serverless functions?
3. Do you need to migrate machines that have a higher capacity or special hardware requirements that are not supported by one of the Azure VM sizes?
4. Are some workloads suitable for Microsoft’s Office 365 environment and not for Azure?

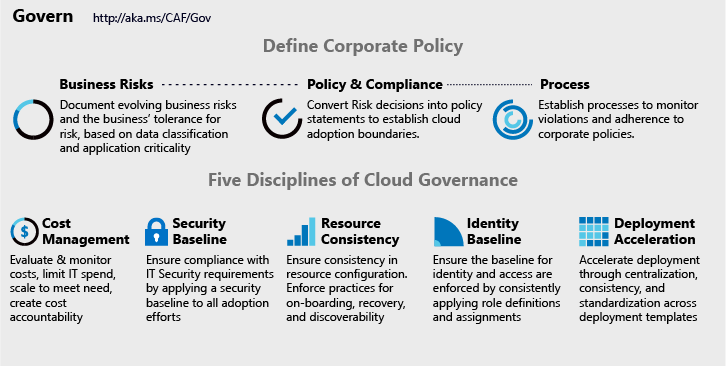
## Migration: Deployment

Azure Adopt end to end deployment / migration detail steps can be found in the Azure Deployment Documentation. [CAF Server Migration Deployment Guide](https://microsoft.sharepoint.com/:w:/t/CAFEnablementKitDevelopment/EcVNqmA2DJBIq6JfQKJ7_94BxupbLzooC5lGYZ2boK2mbg?e=yKj5Mc)

# Govern

The Cloud migration creates new technologies that support business and also changes the way on how those technologies are adopted, managed and governed.

For organizations with existing policies that govern on-premises IT environments, cloud governance should complement those policies. However, 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.

Govern in cloud adoption is an iterative process and span across all cloud adoption phases. [Govern methodology](https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/govern/methodology) need to be considered starting form early strategy stage and then all other phases of the adoption.

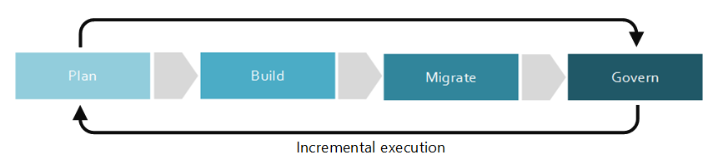
**Corporate policies**: Corporate policies drive cloud governance. Governance focuses on specific aspects of corporate policy:

1. Business risks: Identifying and understanding corporate risks.
2. Policy and compliance: Converting risks into policy statements that support any compliance requirements.
3. Processes: Ensuring adherence to the stated policies.

**Policy Disciplines**: There are 5 disciplines of Cloud Governance that support the corporate policies.

1. Cost Management
2. Security Baseline
3. Resource Consistency
4. Identity Baseline
5. Deployment Acceleration

All the above Cloud Governance disciplines follows the below workflow to meet the corporate policies. Below is the incremental approach for Cloud Governance



**Cost Management Policy**

Apply the cost management across the enterprise cloud governance and cloud operation function. All cost management decisions result in a change to the assets which support a workload. Best practice Azure Security policy for cost management that includes costing and sizing of resources hosted in Azure Cloud Environment.

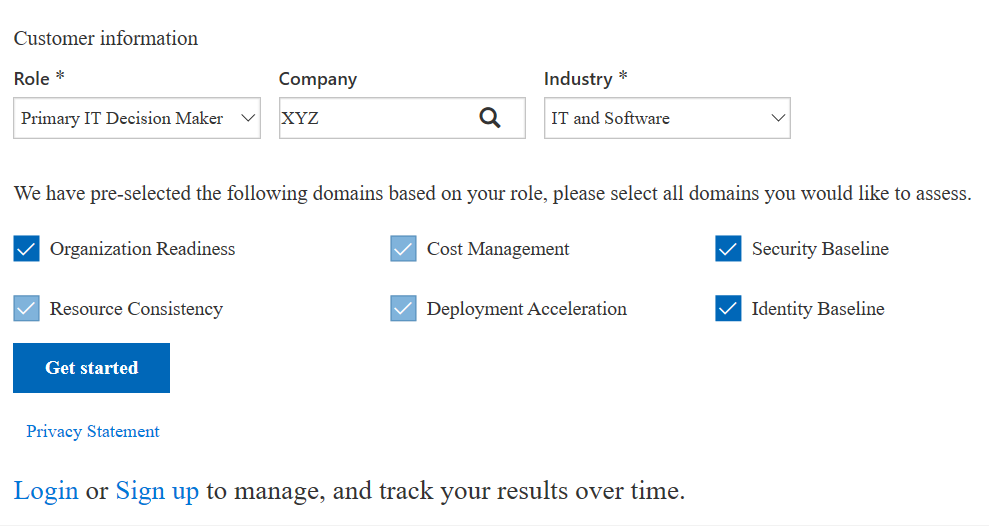
Once the tag policies above are created, join them into a single initiative for tag governance and assign them to a management group or subscription. The initiative and included policies then evaluate compliance of existing resources and alters requests for new or updated resources that match the if property in the policy rule. However, the policy doesn't automatically update existing non-compliant resources with the defined tag changes.

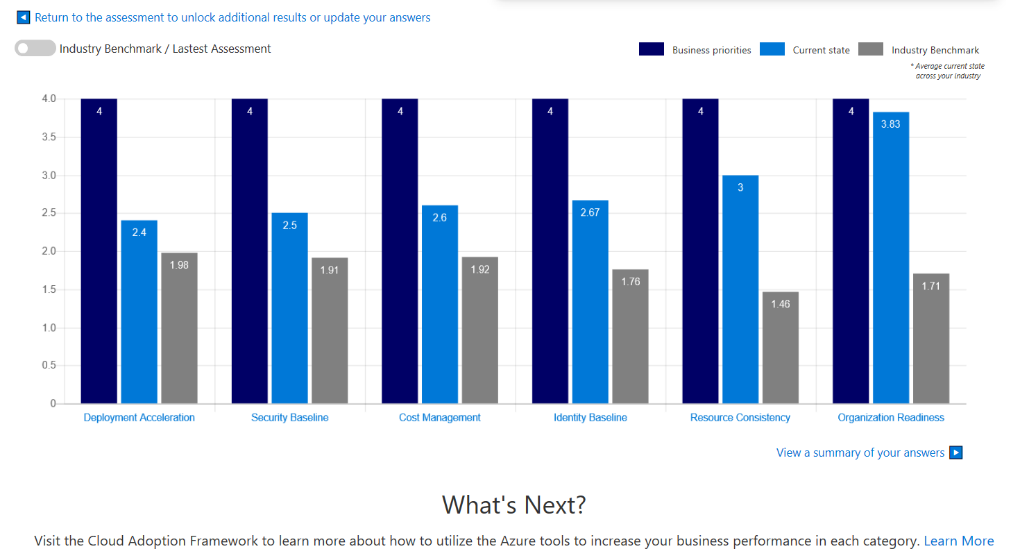
Below is the list of Azure Native Tools to help in policies and processes that support the cost management,

|  |  |
| --- | --- |
| **Tool** | [**Azure Cost Management**](https://docs.microsoft.com/azure/cost-management-billing/cost-management-billing-overview) |
| Enterprise Agreement required? | No |
| Budget control | Yes |
| Monitor spending on single resource | Yes |
| Monitor spending across multiple resources | Yes |
| Control spending on single resource | Yes |
| Enforce spending across multiple resources | Yes |
| Enforce accounting metadata on resources | No |
| Monitor and detect trends | Yes |
| Detect spending anomalies | Yes |
| Socialize deviations | Yes |

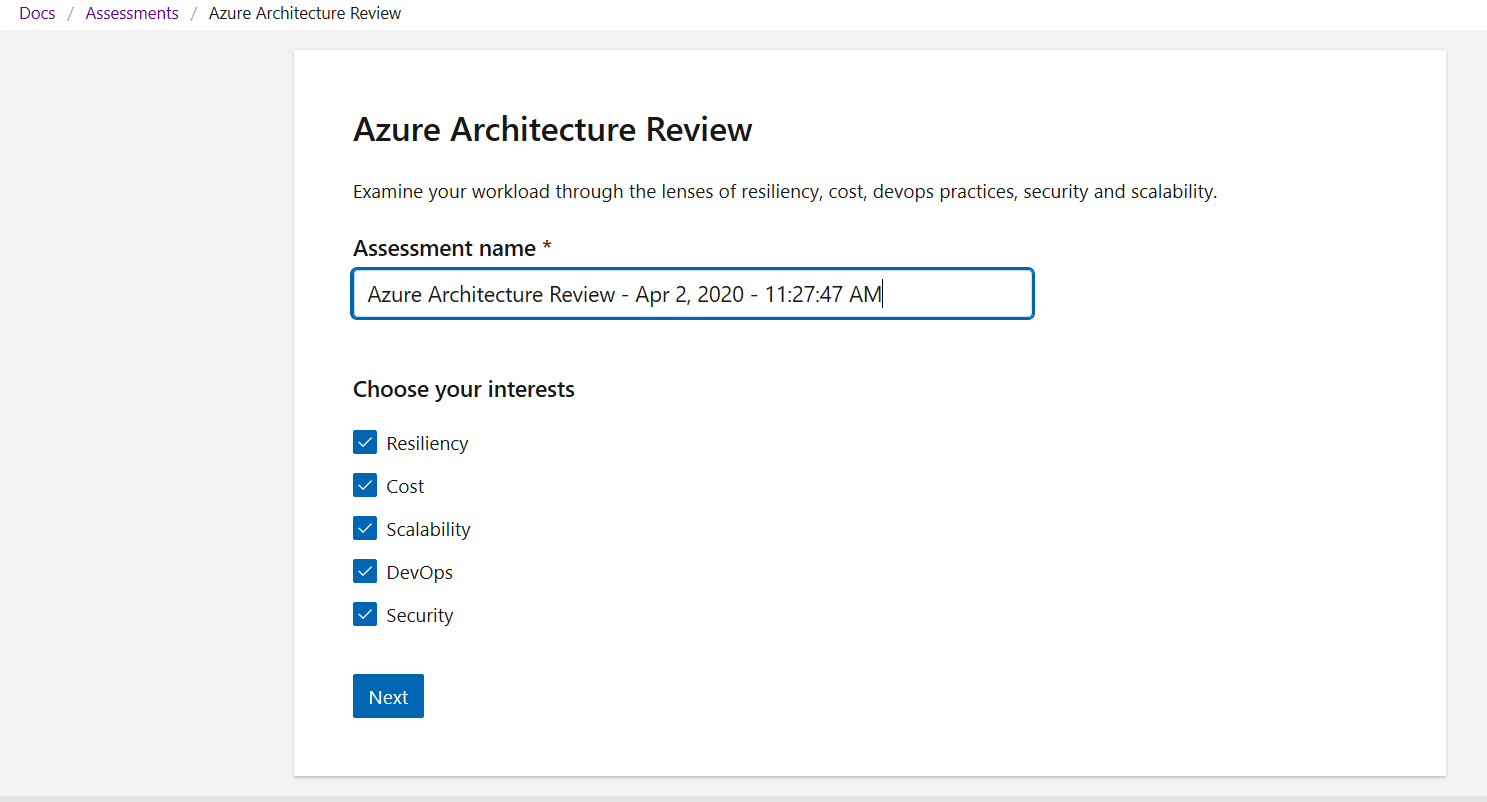
Below features in Azure allow implementation of the corporate policies and governance disciplines. In subsequent sections we will look at these features in detail.

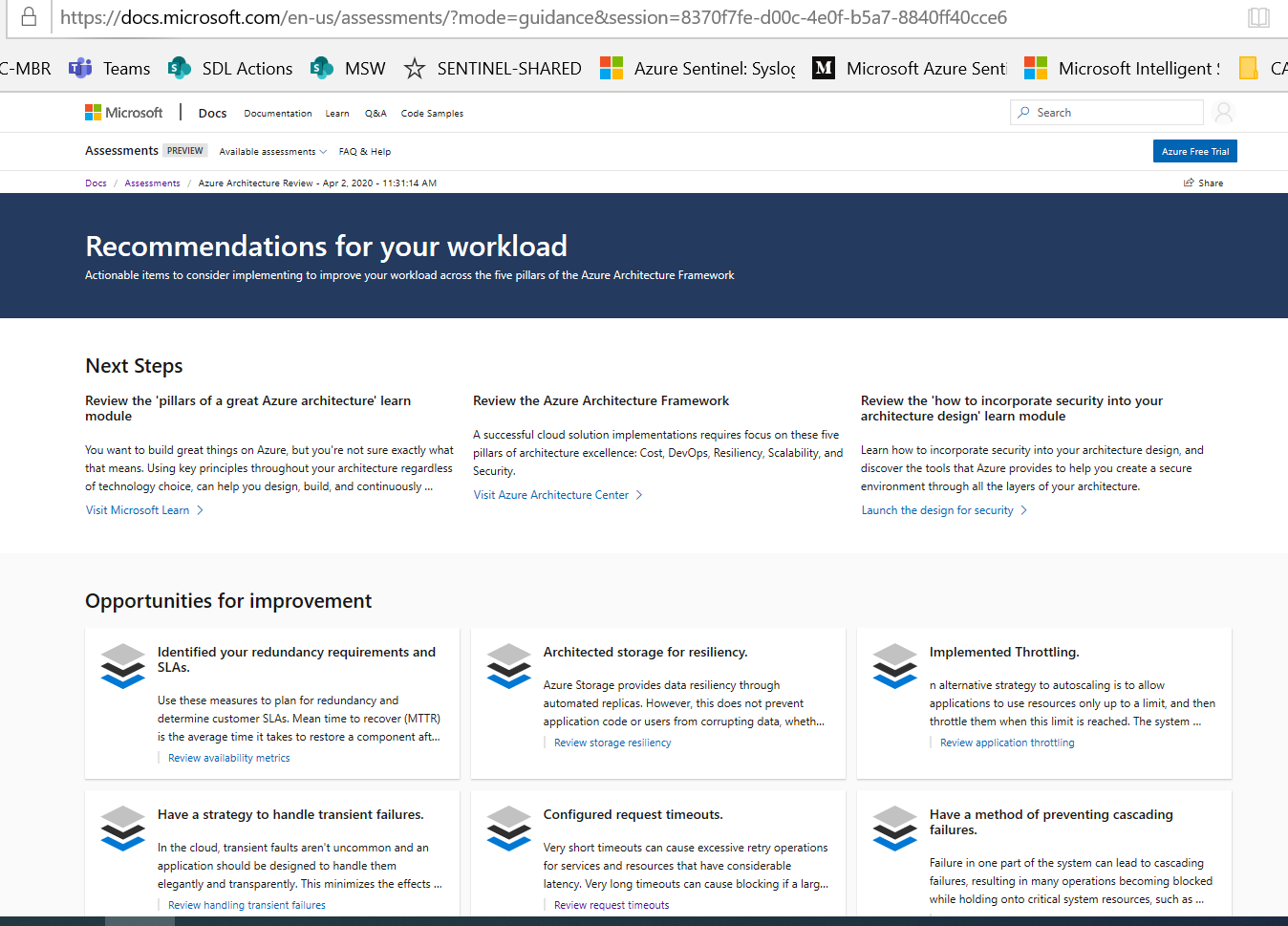
1. Organize Resources
2. Manage access
3. Manage costs
4. Governance, security and compliance
5. Monitoring and reporting

During planning and digital asset discovery one should know governance benchmark based on existing enterprise policies and specific cloud adoption task e.g. workload migration to cloud. [Cloud Adoption Framework Governance Benchmark Tool](https://www.cafbaseline.com/) is the starting point to understand current state and gaps from the governance point of view across all 6 key cloud adoption framework domains. It provides a personalized report that outlines the difference between your current state and business priorities, and tailored resources to help you get started.



One more assessment tools can help expediate decision making is [Azure Architecture Review](https://docs.microsoft.com/en-us/assessments/). [Azure Architecture Review](https://docs.microsoft.com/en-us/assessments/) examine workload through the lenses of resiliency, cost, devops practices, security and scalability and provide detailed recommendation report



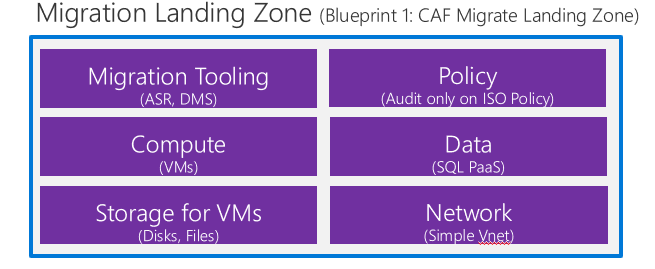


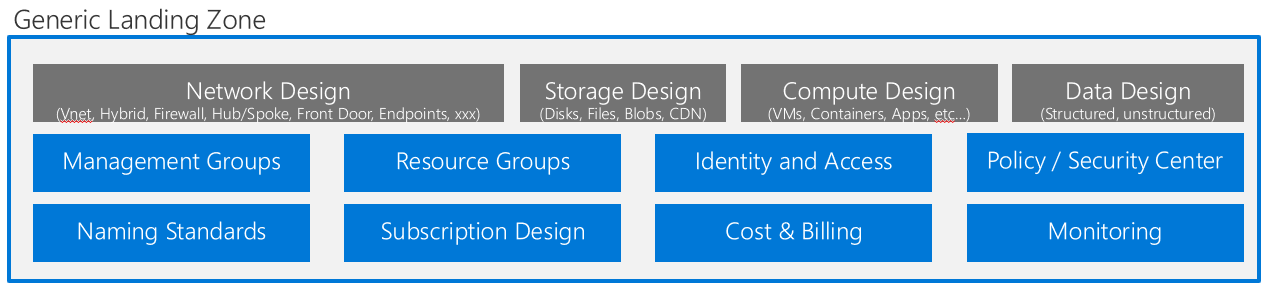
These tools help in overall understanding of the governance domains based on as is environment and to be state in the cloud adoption journey. These assessments can be iterative based on who is performing and for which cloud adoption task or workload. Enterprises can decide to bring in all relevant stakeholders together to perform these assessments.

[Cloud governance foundation](https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/govern/initial-foundation)lightweight starting point is called a minimum viable product (MVP) for governance and the details can vary based on governance consideration for the work at hand or specific workload. Cloud adoption framework provides [cloud governance guides](https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/govern/guides/) which explains various consideration in detail related to specific type of enterprise. There are five disciplines [Cost Management](https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/govern/cost-management/), [Security baseline](https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/govern/security-baseline/), [Identity baseline](https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/govern/identity-baseline/), [Resource consistency](https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/govern/resource-consistency/), [Deployment acceleration](https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/govern/deployment-acceleration/) which need to be considered while deciding governance dependencies and considerations needed for cloud adoption moving to desired state.

Governance Tools -

|  |  |
| --- | --- |
| Risks, compliance, Process | Azure Monitor |
| Cost Management | Azure Blueprint, Azure Policy, Azure cost management, Azure Advisor, Azure EA Content Pack |
| Security baseline | Azure Blueprint, Azure Policy, Azure Security Center, Encryption, Hybrid Identity, Azure Networking, Azure Automation |
| Resource Consistency | Azure Blueprint, Azure Policy, Azure Monitor, Azure Advisor, Resource Manager templates, Resource Graph, Management Groups |
| Identity Baseline | Azure Blueprint, Azure AD, Azure AD B2B, Azure AD B2C, Directory Federation, Directory Replication |
| Deployment Acceleration | Azure Blueprint, Azure Policy, Resource Grouping and Tagging, Resource Manager Templates, Azure Advisor, Azure DevOps, Azure Site Recovery, Azure Backup, Azure Automation |





Refer to Ready section for details on how to use governance tools.

## Governance, Security and Compliance

After planning required resources for migration and managing to access to those resources, Data governance comes into picture. Once the governance strategy is ready we can use the following azure services to automate the organization’s governance decisions:

[**Azure Policy**](https://docs.microsoft.com/en-us/azure/governance/policy/overview)

Azure Policy is a service that you use to create, assign, and manage policies. These policies enforce rules on your resources, so those resources stay compliant with your corporate standards and service level agreements.

Azure Policy scans your resources to identify resources that aren't compliant with the policies you implement. For example, you can have a policy to allow only a specific virtual machine (VM) size to run in your environment. When you implement this policy, it evaluates existing VMs in your environment and any new VMs that are deployed. The policy evaluation generates compliance events for you to use for monitoring and reporting.

Consider common policies to:

* Enforce tagging for resources and resource groups.
* Restrict regions for deployed resources.
* Restrict expensive SKUs for specific resources.
* Audit use of important optional features like Azure-managed disks.

Refer to this [link](https://docs.microsoft.com/en-us/azure/governance/policy/assign-policy-portal) to create policy using Azure portal.

Azure Policy Objects

* Policy definition
* Initiative definition
* Assignments

***Policy definition***

Every policy definition has conditions under which it's enforced. And, it has a defined effect that takes place if the conditions are met. Below table lists the built-in default policies.

|  |  |  |
| --- | --- | --- |
| Policy | Purpose | Value for the use case |
| Allowed Storage Account SKUs | Determines if a storage account being deployed is within a set of SKU sizes. Its effect is to deny all storage accounts that don't adhere to the set of defined SKU sizes. | Allow geo redundant storage only in production subscription. Dev and QA can have local redundant storage. |
| Allowed Resource Type | Defines the resource types that you can deploy. Its effect is to deny all resources that aren't part of this defined list. | Allow only VM, storage, managed instance, SQL, VNet in production. Additional resources can be created in dev and QA. |
| Allowed Locations | Restricts the available locations for new resources. Its effect is used to enforce your geo-compliance requirements. | Restrict Dev and QA to West US. Restrict production to US, Canada and Europe. |
| Allowed Virtual Machine SKUs | Specifies a set of virtual machine SKUs that you can deploy. | Allow high performance compute SKUs only to production. |
| Add a tag to resources | Applies a required tag and its default value if it's not specified by the deploy request. | Look for the tag Cost Center in resource group. If it is not present then create the tag ‘Cost Center’ with value ‘Undefined’. |

***Initiative definition***

An initiative definition is a collection of policy definitions that are tailored towards achieving a singular overarching goal. Initiative definitions simplify managing and assigning policy definitions. They simplify by grouping a set of policies as one single item.

For the use case, create an initiative titled ‘Enable Monitoring in Azure Security Center’, with a goal to monitor all the available security recommendations in your Azure Security Center. Add the below policies to this initiative.

|  |  |
| --- | --- |
| Policy | Purpose |
| Monitor unencrypted SQL Database in Security Center | For monitoring unencrypted SQL databases and servers. |
| Monitor OS vulnerabilities in Security Center | For monitoring servers that don't satisfy the configured baseline. |
| Monitor missing Endpoint Protection in Security Center | For monitoring servers without an installed endpoint protection agent. |

***Assignments***

An assignment is a policy definition or initiative that has been assigned to take place within a specific scope. This scope could range from a management group to an individual resource. The term scope refers to all the resources, resource groups, subscriptions, or management groups that the definition is assigned to. Assignments are inherited by all child resources. However, you can exclude a subscope from the assignment.

For the use case apply the below assignments.

* Assign a definition that prevents the creation of networking resources in subscription scope.
* Exclude networking resource group from subscription scope. Then grant access to this networking resource group to networking team.

***Azure Blueprints***

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 to speed up development and delivery.

Azure Blueprints makes it possible for development teams to rapidly build and stand up new environments with trust they're building within organizational compliance with a set of built-in components -- such as networking -- to speed up development and delivery.

In our case let’s say we have created a blue print for our migration process which will consist of all the artifacts (Resource group, policy assignment, role assignment, etc) required to create environment. Now at some point if you want to make any changes in this environment then blueprint is the only thing that you need to look. Blueprints can be saved and reuse for the purpose like creating new database.

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.

Refer to this [link](https://docs.microsoft.com/en-in/azure/governance/blueprints/create-blueprint-portal) for steps to create and assign blueprint through Azure portal.

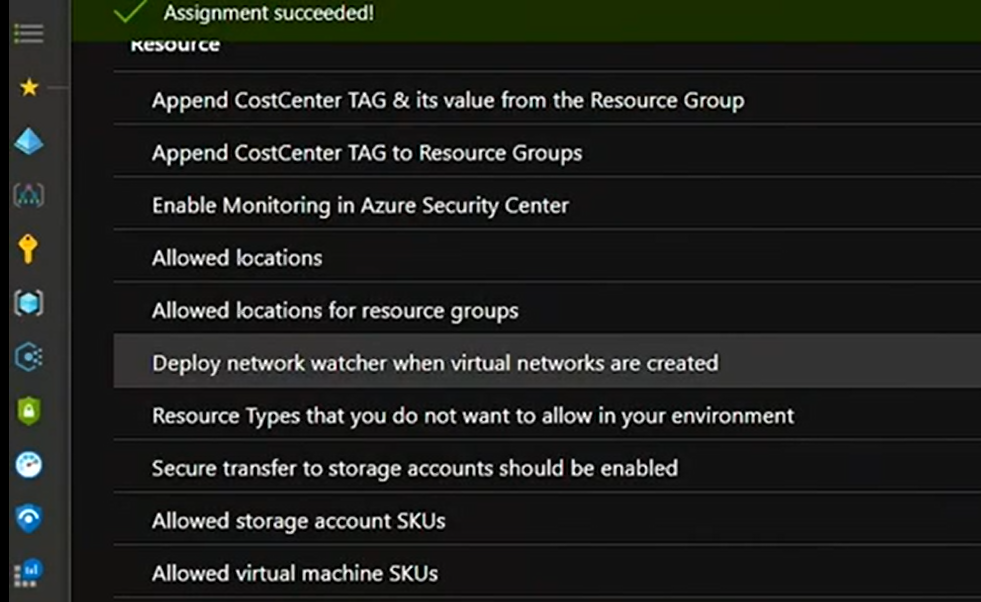
Azure Blueprints provides sample blueprints which are production quality and ready to deploy today to assist in meeting various compliance needs. Refer to this [link](https://docs.microsoft.com/en-in/azure/governance/blueprints/samples/#standards-based-blueprint-samples) for list of all standards-based blueprint samples.

For the use case, apply the below standard-based blueprints.

|  |  |
| --- | --- |
| Standard-based blueprint | Purpose |
| [CIS Microsoft Azure Foundations Benchmark](https://docs.microsoft.com/en-in/azure/governance/blueprints/samples/cis-azure-1.1.0/) | Provides a set of policies to help comply with CIS Microsoft Azure Foundations Benchmark recommendations. |
| [CAF Foundation](https://docs.microsoft.com/en-in/azure/governance/blueprints/samples/caf-foundation/) | Provides a set of controls to help you manage your cloud estate in alignment with the [Microsoft Cloud Adoption Framework for Azure (CAF)](https://docs.microsoft.com/en-us/azure/architecture/cloud-adoption/governance/journeys/index). |
| [ISO 27001 App Service Environment/SQL Database workload](https://docs.microsoft.com/en-in/azure/governance/blueprints/samples/iso27001-ase-sql-workload/) | For monitoring servers without an installed endpoint protection agent. |

The above 3 blueprints have lots of steps. Below is a callout to few useful steps from the blueprints that are applicable to the use case.

1. An Azure Key Vault instance used to host secrets used for the VMs deployed in the shared services environment
2. Deploy Log Analytics is deployed to ensure all actions and services log to a central location from the moment you start your secure deployment in to Storage Accounts for diagnostic logging
3. Deploy Azure Security Center (standard version) provides threat protection for your migrated workloads
4. Tagging (CostCenter) applied to resources groups
5. Append resources in resource group with the CostCenter Tag
6. Allowed Azure Region for Resources and Resource Groups
7. Allowed Storage Account SKUs (refer to section Policy definition)
8. Allowed Azure VM SKUs (refer to section Policy definition)
9. Require Network Watch to be deployed
10. Require Azure Storage Account Secure transfer Encryption
11. Deny resource types (refer to section Policy definition)
12. Audit external accounts with owner permissions on a subscription
13. Audit external accounts with write permissions on a subscription
14. Audit missing blob encryption for storage accounts
15. Transparent Data Encryption on SQL databases should be enabled
16. Audit diagnostic setting
17. Audit SQL server level Auditing settings
18. Auditing should be enabled on advanced data security settings on SQL Server
19. Monitor possible app Whitelisting in Azure Security Center
20. Monitor missing Endpoint Protection in Azure Security Center
21. Monitor missing system updates in Azure Security Center
22. Monitor OS vulnerabilities in Azure Security Center
23. Monitor SQL vulnerability assessment results in Azure Security Center
24. Monitor VM Vulnerabilities in Azure Security Center
25. Monitor permissive network access in Azure Security Center
26. Monitor unprotected network endpoints in Azure Security Center
27. Monitor unprotected web application in Azure Security Center
28. Audit unrestricted network access to storage accounts
29. Ensure that multi-factor authentication is enabled for all privileged users
30. Ensure that no custom subscription owner roles are created
31. Ensure that 'Automatic provisioning of monitoring agent' is set to 'On'
32. Ensure that standard pricing tier is selected
33. Ensure ASC Default policy setting "Monitor OS Vulnerabilities" is not "Disabled"
34. Ensure ASC Default policy setting "Monitor Endpoint Protection" is not "Disabled"
35. Ensure ASC Default policy setting "Monitor Disk Encryption" is not "Disabled"
36. Ensure ASC Default policy setting "Monitor Web Application Firewall" is not "Disabled"
37. Ensure ASC Default policy setting "Enable Next Generation Firewall(NGFW) Monitoring" is not "Disabled"
38. Ensure ASC Default policy setting "Monitor Storage Blob Encryption" is not "Disabled"
39. Ensure ASC Default policy setting "Monitor JIT Network Access" is not "Disabled"
40. Ensure ASC Default policy setting "Monitor Adaptive Application Whitelisting" is not "Disabled"
41. Ensure ASC Default policy setting "Monitor SQL Encryption" is not "Disabled



[**Azure security center:**](https://docs.microsoft.com/en-us/azure/security-center/)

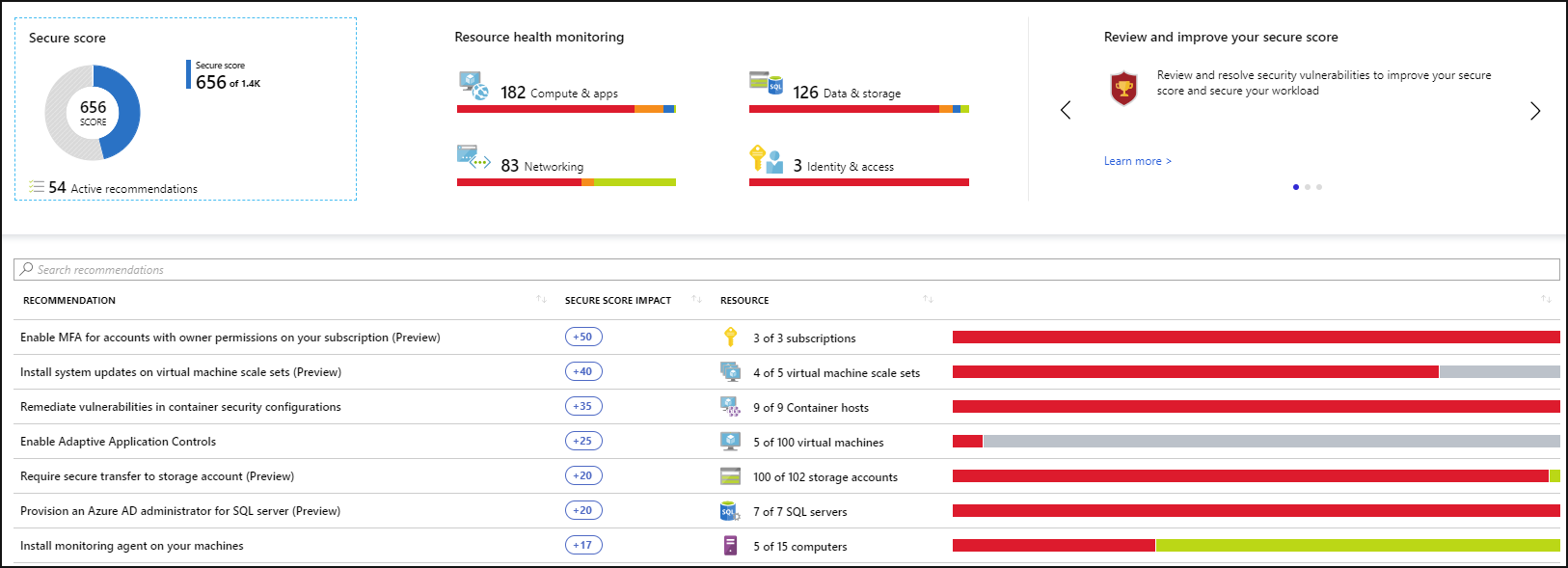
Azure Security Center plays an important part in your governance strategy. It helps you stay on top of security because it:

* Provides a unified view of security across your workloads.
* Collects, searches, and analyzes security data from a variety of sources, which includes firewalls and other partner solutions.
* Provides actionable security recommendations to fix issues before they can be exploited.
* Can be used to apply security policies across your hybrid cloud workloads to ensure compliance with security standards

Many of the security features, like security policy and recommendations, are available for free. Some of the more advanced features, like just-in-time VM access and hybrid workload support, are available under the Security Center standard tier. Just-in-time VM access can help reduce the network attack surface by controlling access to management ports on Azure VMs.

For the use case, onboard the subscription to Security Center to strengthen security and protect against threats to SQL, VMs, storage, VNets and other resources in the subscription. Refer to this [link](https://docs.microsoft.com/en-us/azure/security-center/security-center-get-started) for steps to onboard a subscription to Security Center.

The Secure Scores are associated with each recommendation received to help understand how important each recommendation is to overall security posture. This is crucial in enabling to prioritize security work.



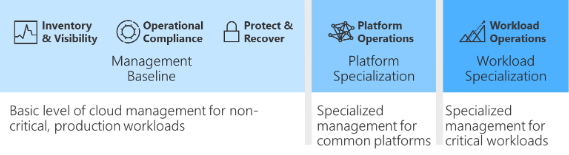
Security Center's threat protection enables to detect and prevent threats at the Infrastructure as a Service (IaaS) layer, non-Azure servers as well as for Platforms as a Service (PaaS) in Azure.

CAF Server Migration Govern Security Policy Consolidation list available in the [Link](https://microsoft.sharepoint.com/:x:/t/CAFEnablementKitDevelopment/ETUQnY3_0JRAhQA1xr5mn4gB0IMva6Q6c81sT4QQ-Cbucg?e=S8MGcc)

CAF Server Migration Govern Security Policy documentation and automation script available in the link

# Manage

Azure Manage outlines on how to establish tooling for a management baseline. It also outlines ways to extend the baseline or build resiliency beyond the baseline.



Minimum management 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 management baseline

* 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.

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.

This is perhaps the most important stage—ongoing operations in the cloud. Beyond the regular operational considerations, in a public cloud environment, you will have a few new elements to consider.

Key considerations for the secure and manage stage:

1. Security—understand the security posture of the new cloud-based application, test to ensure security measures are working, and respond to anomalies and incidents. Become familiar with Azure’s comprehensive security recommendations and tools.
2. Data protection—put protective measures in place—[backup](https://cloud.netapp.com/blog/5-considerations-before-you-backup-on-azure), [disaster recovery](https://cloud.netapp.com/blog/the-importance-of-defining-your-cloud-based-disaster-recovery-strategy), encryption and other measures suitable for your compliance requirements and business risks. Azure provides multiple services and mechanisms to protect your data.
3. Monitoring— recognize that cloud environments are dynamic, and performance is not static and not guaranteed. Monitor performance of compute and data services and use tools like the Azure Traffic Manager, NewRelic or AppDynamics to perform real-user monitoring.

## Inventory and visibility

Collecting proper operational data is vital when making decisions about operations. Cloud management teams must understand what is managed and how well those assets are operated. 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 |
| DNS monitoring | DNS Analytics | Security, performance, and operations of DNS |

## Operational compliance

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 |

## Protect and recover

Protect and recover 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. |

Refer to Ready section for details on how to use manage tools.

## Monitoring and Reporting

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. With Microsoft Azure monitoring, you can:

* Discover Azure Virtual machines under an Azure subscription.
* Find the number of VMs that are provisioned and running.
* View the status and configuration information of all the discovered resources.
* Collect and monitor performance metrics (CPU, Memory, Disk, Network, Thread & Process count, .Net CLR metrics).
* Collect and monitor Disk Utilization, Disk IO statistics, Network interface details by enabling Guest OS configuration.

Below are the tools that can be used for monitoring and reporting:

* Azure Monitor: 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.
* Azure Service Health: Azure Service Health provides a personalized view of the health of the Azure services and regions you use.
* Azure Advisor: Azure Advisor is a free, personalized cloud consultant that helps you follow and implement best practices for Azure deployments.
* Azure Security Center: Azure Security Center also plays an important part in your monitoring strategy. It can help you monitor the security of your machines, networks, storage, data services, and applications.

In our case these tools can also be extended to monitor On-premises Infrastructure Physical and Virtual Server which will help us to optimize the existing servers before we start the migration process.

**Azure Monitor**

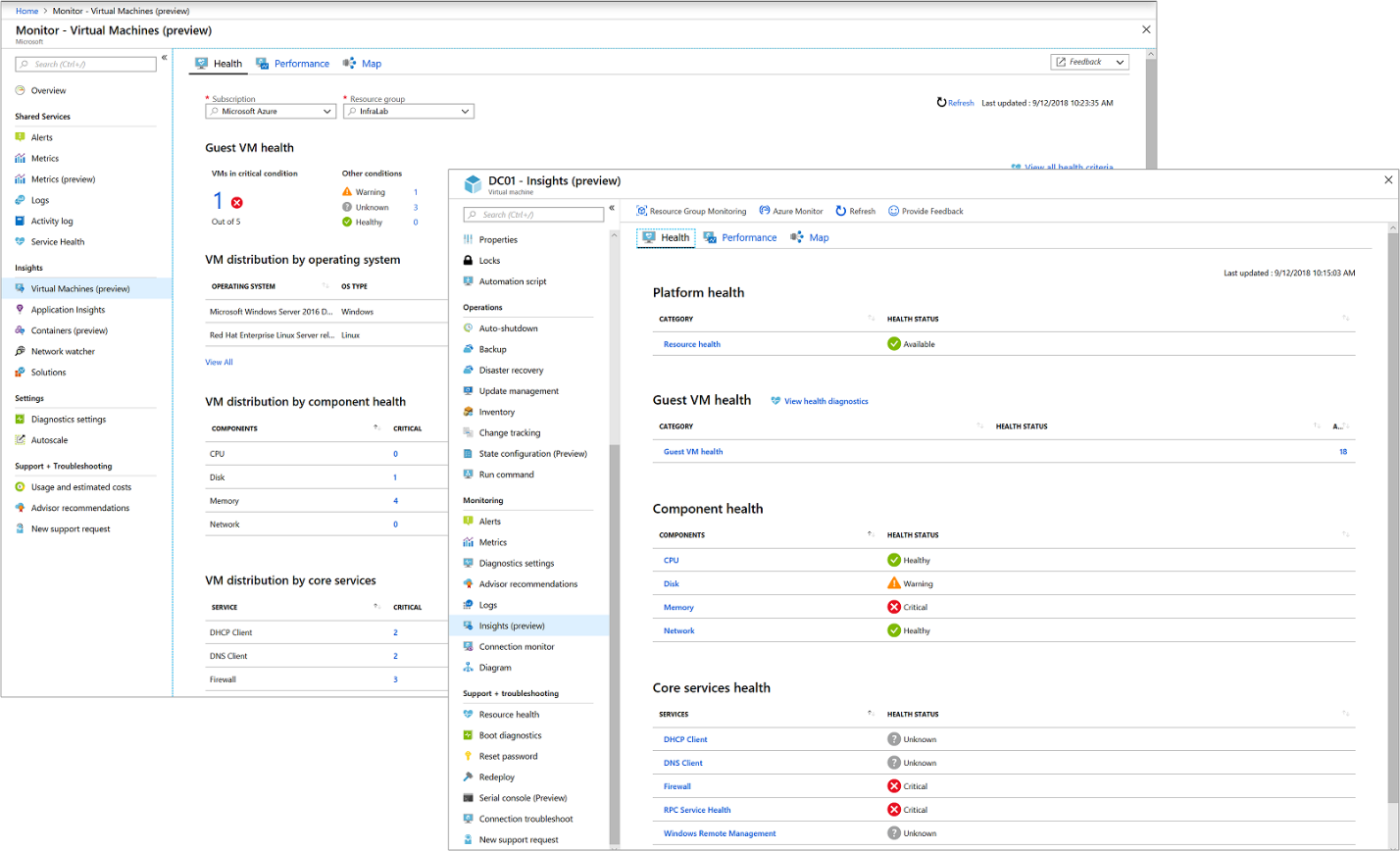
Azure Monitor maximizes the availability and performance of your applications and services by delivering a comprehensive solution for collecting, analyzing, and acting on telemetry from your cloud and on-premises environments. It helps you understand how your applications are performing and proactively identifies issues affecting them and the resources they depend on.

Just a few examples of what you can do with Azure Monitor include:

* Detect and diagnose issues across applications and dependencies with [Application Insights](https://docs.microsoft.com/en-us/azure/azure-monitor/app/app-insights-overview).
* Correlate infrastructure issues with [Azure Monitor for VMs](https://docs.microsoft.com/en-us/azure/azure-monitor/insights/vminsights-overview) and [Azure Monitor for Containers](https://docs.microsoft.com/en-us/azure/azure-monitor/insights/container-insights-overview).
* Drill into your monitoring data with [Log Analytics](https://docs.microsoft.com/en-us/azure/azure-monitor/log-query/log-query-overview) for troubleshooting and deep diagnostics.
* Support operations at scale with [smart alerts](https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-smartgroups-overview) and [automated actions](https://docs.microsoft.com/en-us/azure/azure-monitor/platform/alerts-action-rules).
* Create visualizations with Azure [dashboards](https://docs.microsoft.com/en-us/azure/azure-monitor/learn/tutorial-logs-dashboards) and [workbooks](https://docs.microsoft.com/en-us/azure/azure-monitor/app/usage-workbooks).

For the use case you can use Azure Monitor to monitor VMS, SQL, managed instance etc.

Azure Monitor for VMs monitors your Azure virtual machines (VM) at scale by analyzing the performance and health of your Windows and Linux VMs, including their different processes and interconnected dependencies on other resources and external processes. The solution includes support for monitoring performance and application dependencies for VMs hosted on-premises or another cloud provider.



**Azure Service Health**

Azure Service Health provides a personalized view of the health of the Azure services and regions you use. Information about active issues is posted to Service Health to help you understand the impact to your resources. Regular updates keep you informed as the issue is resolved.

Planned maintenance events are also published to Service Health so you'll know about changes that could affect the availability of your resources. Set up Service Health alerts to be notified when service issues, planned maintenance, or other changes might affect the Azure services and regions you use.

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 each of your individual resources.

**Azure Advisor**

Azure Advisor is a free, personalized cloud consultant that helps you follow and implement best practices for Azure deployments. It analyzes your resource configuration and usage telemetry and recommends solutions that can help optimize your environment.

Azure Security Center

Azure Security Center also plays an important part in your monitoring strategy. It can help you monitor the security of your machines, networks, storage, data services, and applications. 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 or other unwanted code and reduces the surface area exposed to brute force and other network attacks.

When Security Center identifies a threat, it triggers a security alert with steps you need to take to respond to an attack. It also provides a report with information about the threat that was detected.

Azure Security Center is offered in two tiers: free and standard. Features like security recommendations are available for free. The standard tier provides additional protection like advanced threat detection and protection across hybrid cloud workloads.

# Appendix A - References

|  |  |
| --- | --- |
| Reference | Description |
| [Azure RBAC](https://docs.microsoft.com/en-us/azure/role-based-access-control/) | Azure role-based access control (Azure RBAC) is a system that provides fine-grained access management of Azure resources. Using Azure RBAC, you can segregate duties within your team and grant only the amount of access to users that they need to perform their jobs. |
| [Microsoft-Cloud-Adoption-Framework-Strategy-and-Plan-Template](https://archcenter.blob.core.windows.net/cdn/fusion/readiness/Microsoft-Cloud-Adoption-Framework-Strategy-and-Plan-Template.docx) | Document decisions as you execute your cloud adoption strategy and plan. |
| <https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/migrate/azure-migration-guide/?tabs=MigrationTools> | Azure Server Migration Tools and resources |
| <https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/plan/suggested-skills> | Azure Server Migration Suggested Skills required |
| Refer to this [link](https://docs.microsoft.com/en-us/azure/azure-monitor/insights/vminsights-enable-overview) for steps to enable monitor for VMs. | Enabling Monitoring for VMs |
| Refer to this [link](https://docs.microsoft.com/en-us/azure/advisor/advisor-get-started) for steps to get starts with Azure Advisor. | Information about Azure Advisor |
| <https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/decision-guides/> | Guidance for Architecture Decision for Azure Server Migration |

# Appendix B: Documentation Revision Table

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Version** | **Changes** | **Author** | **Date** | **Approver** |
| v0.1 | Initial Release | Sushil Darekar | 1st March 2020 | Farida Bharmal |
| v1.0 | Updated documentation | Sushil Darekar | 7th May 2020 | Farida Bharmal |
| v1.1 | Updated documentation included Deployment documentation | Ganesh Pandian | 13th May 2020 | Farida Bharmal |
| v1.1 | Updated documentation included Policy documentation | Ganesh Pandian | 8th Jun 2020 |  |