AZ-900

Thursday, January 21, 2021 11:27 PM

Part 1 - Describe core Azure concepts

Thursday, January 28, 2021 10:09 AM

Introduction to Azure fundamentals

Thursday, January 21, 2021 11:27 PM

Introduction to Azure fundamentals

From <https://docs.microsoft.com/en-in/learn/paths/az-900-describe-cloud-concepts/>

- Introduction4 min
- What is cloud computing?9 min
  - It's the delivery of computing services over the internet, which is otherwise known as the cloud. These services include servers, storage, databases, networking, software, analytics, and intelligence. Cloud computing offers faster innovation, flexible resources, and economies of scale.
- What is Azure?6 min
- Tour of Azure services11 min
- Get started with Azure accounts2 min
- Case study introduction2 min
- Knowledge check3 min
- Summary1 min

From <https://docs.microsoft.com/en-in/learn/paths/az-900-describe-cloud-concepts/>

Introduction

- 4 minutes

Azure is a cloud computing platform with an ever-expanding set of services to help you build solutions to meet your business goals. Azure services range from simple web services for hosting your business presence in the cloud to running fully virtualized computers for you to run your custom software solutions. Azure provides a wealth of cloud-based services like remote storage, database hosting, and centralized account management. Azure also offers new capabilities like AI and Internet of Things (IoT).
In this module, you'll take an entry-level, end-to-end look at Azure and its capabilities. You'll gain a solid foundation for completing the available learning paths for Azure fundamentals.

What is Azure fundamentals?

Azure fundamentals is a series of six learning paths that helps orient you to Azure and its many services and features.
Whether you're interested in Azure's core compute, network, storage, and database services, learning about cloud security best practices, or exploring the cutting edge in IoT and machine learning, think of Azure fundamentals as your curated guide to Azure.

Azure fundamentals includes interactive exercises that give you hands-on experience with Azure. Many exercises provide a temporary Azure environment called the sandbox, which allows you to learn for free and at your own pace.
Technical IT experience is not required; however, having general IT knowledge will help you get the most from your learning experience.

Why should I take Azure fundamentals?

Whether you're just beginning to work with the cloud or you already have cloud experience and are new to Azure, Azure fundamentals provides you with everything you need to get started.
No matter your goals, Azure fundamentals has something for you. Take Azure fundamentals if you:

- Have general interest in Azure or in the cloud.
- Want to earn official certification from Microsoft.

Preparation for Exam AZ-900
The Azure fundamentals learning path series can help you prepare for Exam AZ-900: Microsoft Azure Fundamentals . This exam includes six knowledge domain areas:

AZ-900 Domain Area	Weight
Describe cloud concepts	20-25%
Describe core Azure services	15-20%
Describe core solutions and management tools on Azure	10-15%
Describe general security and network security features	10-15%
Describe identity, governance, privacy, and compliance features	20-25%
Describe Azure cost management and Service Level Agreements	10-15%

TABLE 1

Each domain area maps to a learning path in Azure fundamentals.
The percentages shown indicate the relative weight of each area on the exam. The higher the percentage, the more questions that part of the exam will contain. Be sure to read the exam page for specifics about what skills are covered in each area.
This training helps you develop a broad understanding of Azure. Having real-world experience will help reinforce the concepts so that you're more fully prepared for the exam or to apply your skills on the job.

Learning objectives

After completing this module, you'll be able to:

- Describe the basic concepts of cloud computing.
- Determine whether Azure is the right solution for your business needs.
- Differentiate between the different methods of creating an Azure subscription.

Prerequisites

- You should be familiar with basic computing concepts and terminology.
- Familiarity with cloud computing is helpful but isn't necessary.

From <https://docs.microsoft.com/en-us/learn/modules/intro-to-azure-fundamentals/introduction>

What is cloud computing?

- 9 minutes

Have you ever wondered what cloud computing is? It's the delivery of computing services over the internet, which is otherwise known as the cloud. These services include servers, storage, databases, networking, software, analytics, and intelligence. Cloud computing offers faster innovation, flexible resources, and economies of scale.

Why is cloud computing typically cheaper to use?

Cloud computing is the delivery of computing services over the internet by using a pay-as-you-go pricing model. You typically pay only for the cloud services you use, which helps you:

- Lower your operating costs.
- Run your infrastructure more efficiently.
- Scale as your business needs change.

To put it another way, cloud computing is a way to rent compute power and storage from someone else's datacenter. You can treat cloud resources like you would your resources in your own datacenter. When you're done using them, you give them back. You're billed only for what you use.

Instead of maintaining CPUs and storage in your datacenter, you rent them for the time that you need them. The cloud provider takes care of maintaining the underlying infrastructure for you. The cloud enables you to quickly solve your toughest business challenges, and bring cutting-edge solutions to your users.

Why should I move to the cloud?

The cloud helps you move faster and innovate in ways that were once nearly impossible. In our ever-changing digital world, two trends emerge:

- Teams deliver new features to their users at record speeds.
- Users expect an increasingly rich and immersive experience with their devices and with software.

Software releases were once scheduled in terms of months or even years. Today, teams release features in smaller batches that are often scheduled in days or weeks. Some teams even deliver software updates continuously--sometimes with multiple releases

within the same day.
Think of all the ways you interact with devices that you couldn't do a few years ago. Many devices can recognize your face and respond to voice commands. Augmented reality changes the way you interact with the physical world. Household appliances are even beginning to act intelligently. These technologies are only a few examples, and many of them are powered by the cloud.
To power your services and deliver innovative and novel user experiences more quickly, the cloud provides on-demand access to:

- A nearly limitless pool of raw compute, storage, and networking components.
- Speech recognition and other cognitive services that help make your application stand out from the crowd.
- Analytics services that deliver telemetry data from your software and devices.

What are some cloud computing advantages?

There are several benefits that a cloud environment has over a physical environment. For example, cloud-based applications employ a myriad of related strategies:

- Reliability: Depending on the service-level agreement that you choose, your cloud-based applications can provide a continuous user experience with no apparent downtime even when things go wrong.
- Scalability: Applications in the cloud can be scaled in two ways, while taking advantage of autoscaling:
- *Vertically*: Computing capacity can be increased by adding RAM or CPUs to a virtual machine.
- *Horizontally*: Computing capacity can be increased by adding instances of a resource, such as adding more virtual machines to your configuration.
- Elasticity: Cloud-based applications can be configured to always have the resources they need.
- Agility: Cloud-based resources can be deployed and configured quickly as your application requirements change.
- Geo-distribution: Applications and data can be deployed to regional datacenters around the globe, so your customers always have the best performance in their region.
- Disaster recovery: By taking advantage of cloud-based backup services, data replication, and geo-distribution, you can deploy your applications with the confidence that comes from knowing that your data is safe in the event that disaster should occur.

What are cloud service models?

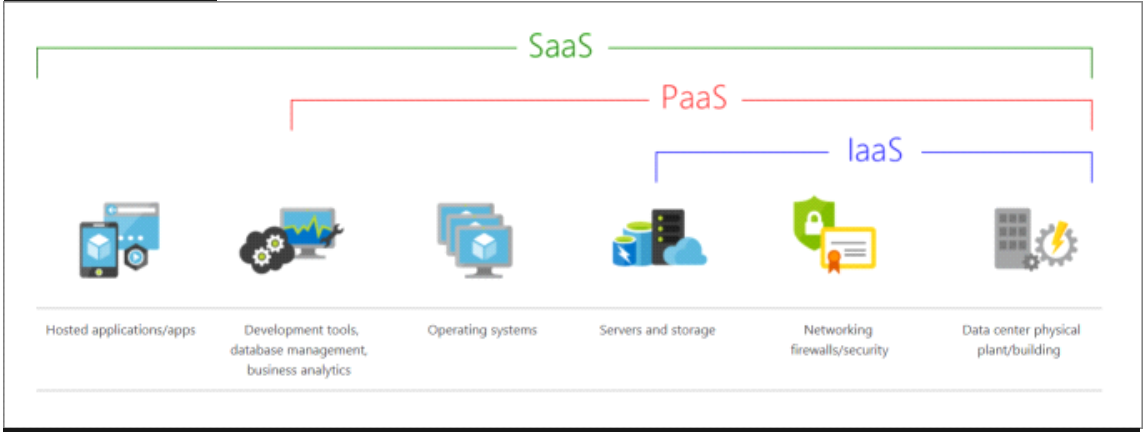
Cloud computing falls into one of the following computing models. If you've been around cloud computing for a while, you've probably seen the terms infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS) for the different cloud service models. These models define the different level of shared

responsibility that a cloud provider and cloud tenant are responsible for.

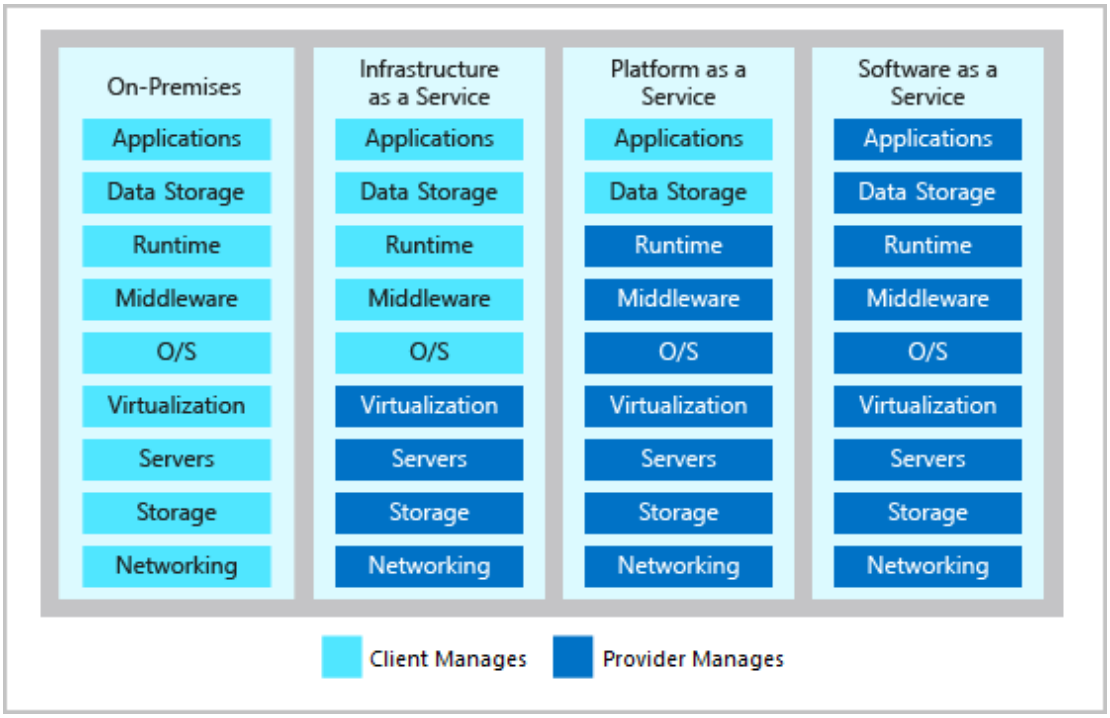
Computing model	Description
IaaS	This cloud service model is the closest to managing physical servers. A cloud provider keeps the hardware up to date, but operating system maintenance and network configuration is left to the cloud tenant. For example, Azure virtual machines are fully operational virtual compute devices running in Microsoft's datacenters. An advantage of this cloud service model is rapid deployment of new compute devices. Setting up a new virtual machine is considerably faster than procuring, installing, and configuring a physical server.
PaaS	This cloud service model is a managed hosting environment. The cloud provider manages the virtual machines and networking resources, and the cloud tenant deploys their applications into the managed hosting environment. For example, Azure App Services provides a managed hosting environment where developers can upload their web applications without having to deal with the physical hardware and software requirements.
SaaS	In this cloud service model, the cloud provider manages all aspects of the application environment, such as virtual machines, networking resources, data storage, and applications. The cloud tenant only needs to provide their data to the application managed by the cloud provider. For example, Office 365 provides a fully working version of Office that runs in the cloud. All that you need to do is create your content, and Office 365 takes care of everything else.

WHAT ARE CLOUD SERVICE MODELS?

The following illustration demonstrates the services that might run in each of the cloud service models.



The following chart illustrates the various levels of responsibility between a cloud provider and a cloud tenant.



What is serverless computing?

Overlapping with PaaS, serverless computing enables developers to build applications faster by eliminating the need for them to manage infrastructure. With serverless applications, the cloud service provider automatically provisions, scales, and manages the infrastructure required to run the code. Serverless architectures are highly scalable and event-driven. They use resources only when a specific function or trigger occurs. In understanding the definition of serverless computing, it's important to note that servers are still running the code. The serverless name comes from the fact that the tasks associated with infrastructure provisioning and management are invisible to the developer. This approach enables developers to increase their focus on the business logic and deliver more value to the core of the business. Serverless computing helps teams increase their productivity and bring products to market faster. It allows organizations to better optimize resources and stay focused on innovation.

What are public, private, and hybrid clouds?

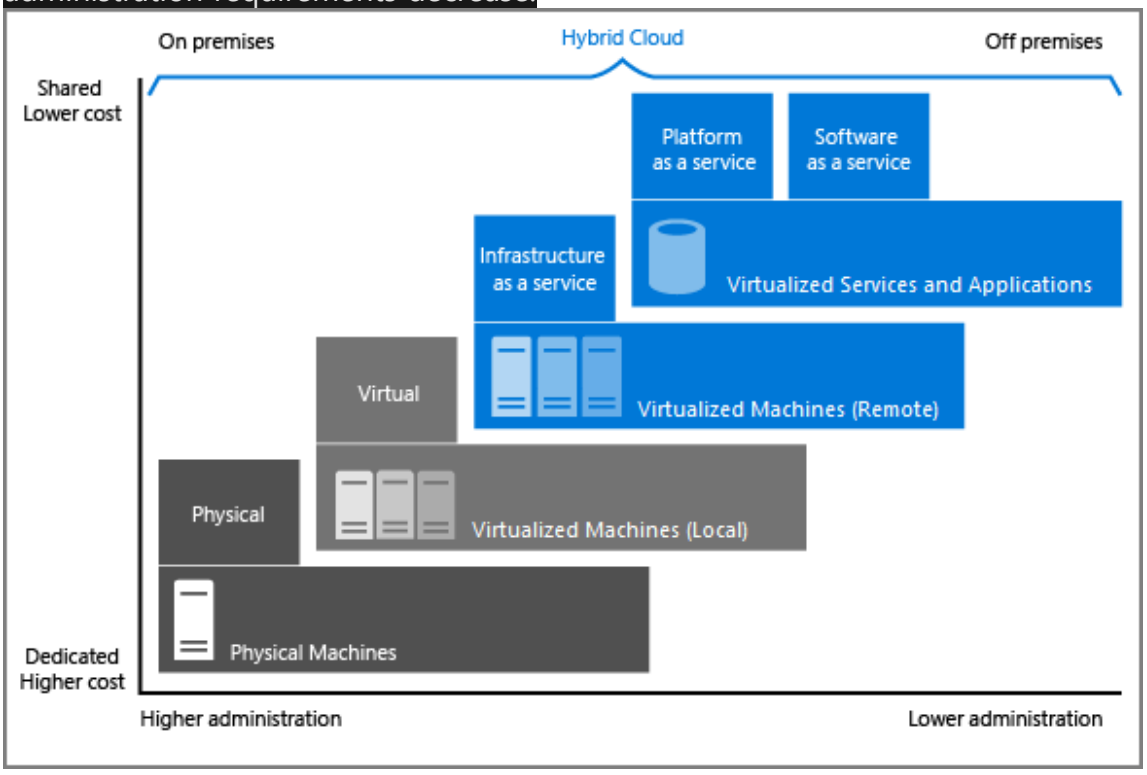
There are three deployment models for cloud computing: *public cloud*, *private cloud*, and *hybrid cloud*. Each deployment model has different aspects that you should consider as you migrate to the cloud.

Deployment model	**Description**
Public cloud	Services are offered over the public internet and available to anyone who wants to purchase them. Cloud resources like servers and storage are owned and operated by a third-party cloud service provider and delivered over the internet.
Private	Computing resources are used exclusively by users from one business or organization. A

cloud	private cloud can be physically located at your organization's on-site datacenter. It also can be hosted by a third-party service provider.
Hybrid cloud	This computing environment combines a public cloud and a private cloud by allowing data and applications to be shared between them.

WHAT ARE PUBLIC, PRIVATE, AND HYBRID CLOUDS?

The following image illustrates several of the cloud computing concepts that are presented in this unit. In this example, several factors are demonstrated when you're considering where to deploy a database server in a hybrid cloud environment. As your resources move from on-premises to off-premises, your costs are reduced, and your administration requirements decrease.



From <https://docs.microsoft.com/en-us/learn/modules/intro-to-azure-fundamentals/what-is-cloud-computing>

What is Azure?

- 6 minutes

Azure is a continually expanding set of cloud services that help your organization meet your current and future business challenges. Azure gives you the freedom to build, manage, and deploy applications on a massive global network using your favorite tools and frameworks.

What does Azure offer?

With help from Azure, you have everything you need to build your next great solution. The following table lists several of the benefits that Azure provides, so you can easily invent with purpose.

Be ready for the future: Continuous innovation from Microsoft supports your development today and your product visions for tomorrow.

Build on your terms: You have choices. With a commitment to open source, and support for all languages and frameworks, build how you want and deploy where you want to.

Operate hybrid seamlessly: On-premises, in the cloud, and at the edge--we'll meet you where you are. Integrate and manage your environments with tools and services designed for a hybrid cloud solution.

Trust your cloud: Get security from the ground up, backed by a team of experts, and proactive compliance trusted by enterprises, governments, and startups.

What can I do with Azure?

Azure provides more than 100 services that enable you to do everything from running

your existing applications on virtual machines to exploring new software paradigms, such as intelligent bots and mixed reality.

Many teams start exploring the cloud by moving their existing applications to virtual machines that run in Azure. Migrating your existing apps to virtual machines is a good start, but the cloud is much more than a different place to run your virtual machines. For example, Azure provides AI and machine-learning services that can naturally communicate with your users through vision, hearing, and speech. It also provides storage solutions that dynamically grow to accommodate massive amounts of data. Azure services enable solutions that aren't feasible without the power of the cloud.

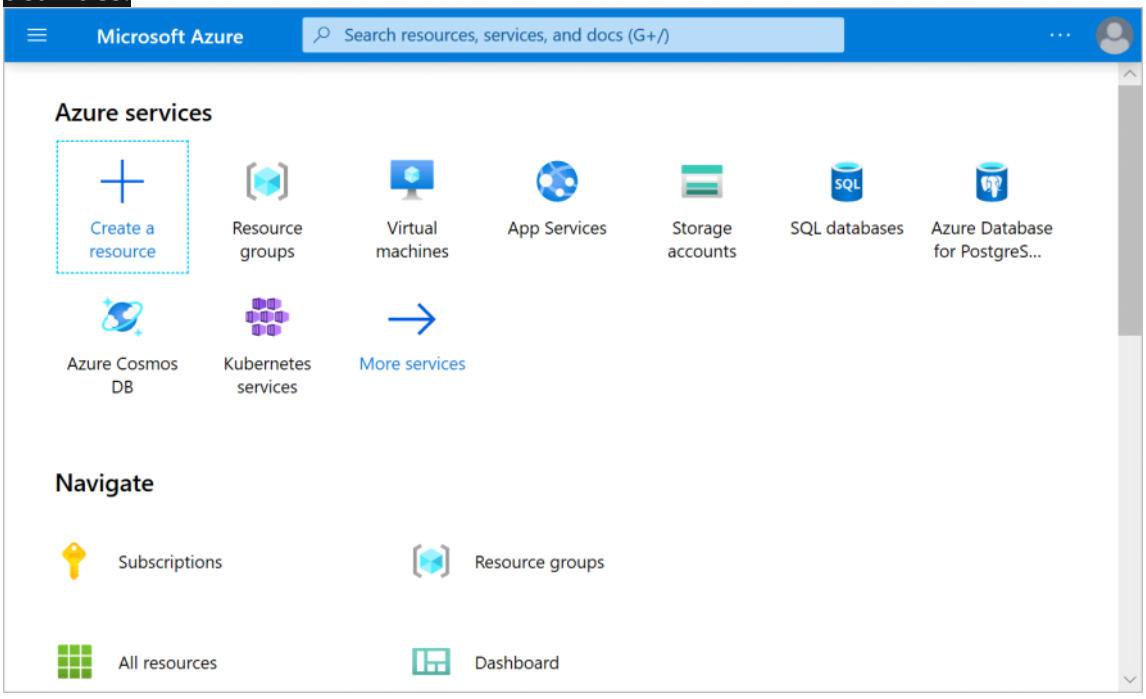
How does Azure work?

What is the Azure portal?

The Azure portal is a web-based, unified console that provides an alternative to command-line tools. With the Azure portal, you can manage your Azure subscription by using a graphical user interface. You can:

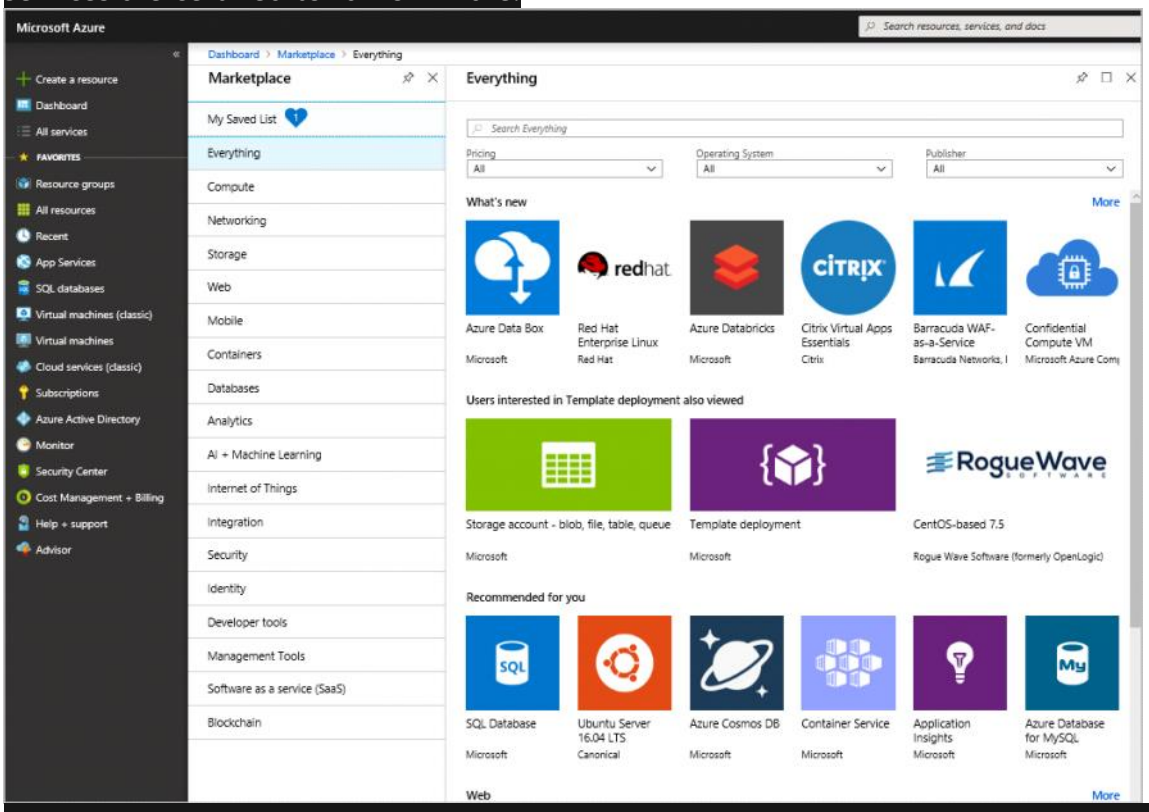
- Build, manage, and monitor everything from simple web apps to complex cloud deployments.
- Create custom dashboards for an organized view of resources.
- Configure accessibility options for an optimal experience.

The Azure portal is designed for resiliency and continuous availability. It maintains a presence in every Azure datacenter. This configuration makes the Azure portal resilient to individual datacenter failures and avoids network slowdowns by being close to users. The Azure portal updates continuously and requires no downtime for maintenance activities.



What is Azure Marketplace?

Azure Marketplace helps connect users with Microsoft partners, independent software vendors, and startups that are offering their solutions and services, which are optimized to run on Azure. Azure Marketplace customers can find, try, purchase, and provision applications and services from hundreds of leading service providers. All solutions and services are certified to run on Azure.



The solution catalog spans several industry categories such as open-source container platforms, virtual machine images, databases, application build and deployment software, developer tools, threat detection, and blockchain. Using Azure Marketplace, you can provision end-to-end solutions quickly and reliably, hosted in your own Azure environment. At the time of writing, there are more than 8,000 listings.
Azure Marketplace is designed for IT pros and cloud developers interested in commercial and IT software. Microsoft partners also use it as a launch point for all joint go-to-market activities.

From <https://docs.microsoft.com/en-us/learn/modules/intro-to-azure-fundamentals/what-is-microsoft-azure>

Tour of Azure services

- 11 minutes

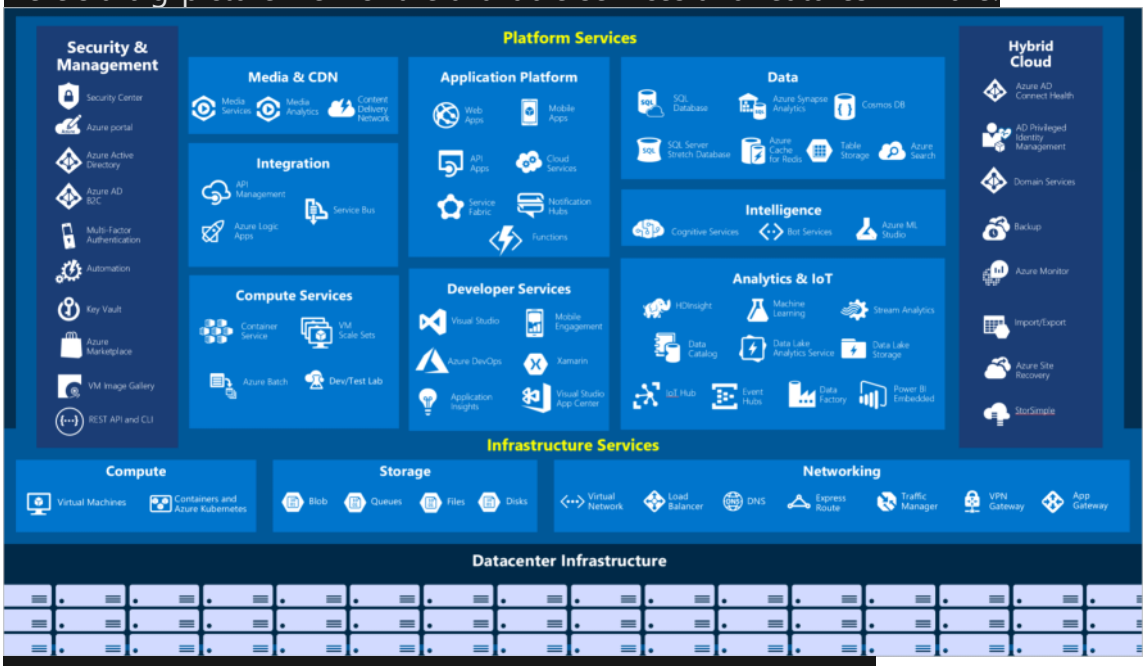
Azure can help you tackle tough business challenges. You bring your requirements,

creativity, and favorite software development tools. Azure brings a massive global infrastructure that's always available for you to build your applications on.
Let's take a quick tour of the high-level services Azure offers.

Azure overview

Azure services

Here's a big-picture view of the available services and features in Azure.



Let's take a closer look at the most commonly used categories:

- Compute
- Networking
- Storage
- Mobile
- Databases
- Web
- Internet of Things (IoT)
- Big data
- AI
- DevOps

Compute

Compute services are often one of the primary reasons why companies move to the Azure platform. Azure provides a range of options for hosting applications and services. Here are some examples of compute services in Azure.

Service name	Service function
Azure Virtual Machines	Windows or Linux virtual machines (VMs) hosted in Azure.
Azure Virtual Machine Scale	Scaling for Windows or Linux VMs hosted in Azure.

Sets	
Azure Kubernetes Service	Cluster management for VMs that run containerized services.
Azure Service Fabric	Distributed systems platform that runs in Azure or on-premises.
Azure Batch	Managed service for parallel and high-performance computing applications.
Azure Container Instances	Containerized apps run on Azure without provisioning servers or VMs.
Azure Functions	An event-driven, serverless compute service.

TABLE 1

Networking

Linking compute resources and providing access to applications is the key function of Azure networking. Networking functionality in Azure includes a range of options to connect the outside world to services and features in the global Azure datacenters. Here are some examples of networking services in Azure.

Service name	Service function
Azure Virtual Network	Connects VMs to incoming virtual private network (VPN) connections.
Azure Load Balancer	Balances inbound and outbound connections to applications or service endpoints.
Azure Application Gateway	Optimizes app server farm delivery while increasing application security.
Azure VPN Gateway	Accesses Azure Virtual Networks through high-performance VPN gateways.
Azure DNS	Provides ultra-fast DNS responses and ultra-high domain availability.
Azure Content Delivery Network	Delivers high-bandwidth content to customers globally.
Azure DDoS Protection	Protects Azure-hosted applications from distributed denial of service (DDOS) attacks.
Azure Traffic Manager	Distributes network traffic across Azure regions worldwide.
Azure ExpressRoute	Connects to Azure over high-bandwidth dedicated secure connections.
Azure Network Watcher	Monitors and diagnoses network issues by using scenario-based analysis.
Azure Firewall	Implements high-security, high-availability firewall with unlimited scalability.
Azure Virtual WAN	Creates a unified wide area network (WAN) that connects local and remote sites.

TABLE 2

Storage

Azure provides four main types of storage services.

Service name	Service function
Azure Blob storage	Storage service for very large objects, such as video files or bitmaps.
Azure File storage	File shares that can be accessed and managed like a file server.

Azure Queue storage	A data store for queuing and reliably delivering messages between applications.
Azure Table storage	A NoSQL store that hosts unstructured data independent of any schema.

TABLE 3

These services all share several common characteristics:

- Durable and highly available with redundancy and replication.
- Secure through automatic encryption and role-based access control.
- Scalable with virtually unlimited storage.
- Managed, handling maintenance and any critical problems for you.
- Accessible from anywhere in the world over HTTP or HTTPS.

Mobile

With Azure, developers can create mobile back-end services for iOS, Android, and Windows apps quickly and easily. Features that used to take time and increase project risks, such as adding corporate sign-in and then connecting to on-premises resources such as SAP, Oracle, SQL Server, and SharePoint, are now simple to include.
Other features of this service include:

- Offline data synchronization.
- Connectivity to on-premises data.
- Broadcasting push notifications.
- Autoscaling to match business needs.

Databases

Azure provides multiple database services to store a wide variety of data types and volumes. And with global connectivity, this data is available to users instantly.

Service name	**Service function**
Azure Cosmos DB	Globally distributed database that supports NoSQL options.
Azure SQL Database	Fully managed relational database with auto-scale, integral intelligence, and robust security.
Azure Database for MySQL	Fully managed and scalable MySQL relational database with high availability and security.
Azure Database for PostgreSQL	Fully managed and scalable PostgreSQL relational database with high availability and security.
SQL Server on Azure Virtual Machines	Service that hosts enterprise SQL Server apps in the cloud.
Azure Synapse Analytics	Fully managed data warehouse with integral security at every level of scale at no extra cost.
Azure Database Migration Service	Service that migrates databases to the cloud with no application code changes.
Azure Cache for Redis	Fully managed service caches frequently used and static data to reduce data and application latency.
Azure Database for MariaDB	Fully managed and scalable MariaDB relational database with high availability and security.

TABLE 4

Web

Having a great web experience is critical in today's business world. Azure includes first-class support to build and host web apps and HTTP-based web services. The following Azure services are focused on web hosting.

Service name	Description
Azure App Service	Quickly create powerful cloud web-based apps.
Azure Notification Hubs	Send push notifications to any platform from any back end.
Azure API Management	Publish APIs to developers, partners, and employees securely and at scale.
Azure Cognitive Search	Deploy this fully managed search as a service.
Web Apps feature of Azure App Service	Create and deploy mission-critical web apps at scale.
Azure SignalR Service	Add real-time web functionalities easily.

TABLE 5

IoT

People are able to access more information than ever before. Personal digital assistants led to smartphones, and now there are smart watches, smart thermostats, and even smart refrigerators. Personal computers used to be the norm. Now the internet allows any item that's online-capable to access valuable information. This ability for devices to garner and then relay information for data analysis is referred to as IoT.
Many services can assist and drive end-to-end solutions for IoT on Azure.

Service name	Description
IoT Central	Fully managed global IoT software as a service (SaaS) solution that makes it easy to connect, monitor, and manage IoT assets at scale.
Azure IoT Hub	Messaging hub that provides secure communications between and monitoring of millions of IoT devices.
IoT Edge	Fully managed service that allows data analysis models to be pushed directly onto IoT devices, which allows them to react quickly to state changes without needing to consult cloud-based AI models.

TABLE 6

Big data

Data comes in all formats and sizes. When we talk about big data, we're referring to *large* volumes of data. Data from weather systems, communications systems, genomic research, imaging platforms, and many other scenarios generate hundreds of gigabytes of data. This amount of data makes it hard to analyze and make decisions. It's

often so large that traditional forms of processing and analysis are no longer appropriate.
Open-source cluster technologies have been developed to deal with these large data sets. Azure supports a broad range of technologies and services to provide big data and analytic solutions.

Service name	Description
Azure Synapse Analytics	Run analytics at a massive scale by using a cloud-based enterprise data warehouse that takes advantage of massively parallel processing to run complex queries quickly across petabytes of data.
Azure HDInsight	Process massive amounts of data with managed clusters of Hadoop clusters in the cloud.
Azure Databricks	Integrate this collaborative Apache Spark-based analytics service with other big data services in Azure.

TABLE 7

AI

AI, in the context of cloud computing, is based around a broad range of services, the core of which is machine learning. Machine learning is a data science technique that allows computers to use existing data to forecast future behaviors, outcomes, and trends. Using machine learning, computers learn without being explicitly programmed. Forecasts or predictions from machine learning can make apps and devices smarter. For example, when you shop online, machine learning helps recommend other products you might like based on what you've purchased. 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.
Here are some of the most common AI and machine learning service types in Azure.

Service name	Description
Azure Machine Learning Service	Cloud-based environment you can use to develop, train, test, deploy, manage, and track machine learning models. It can auto-generate a model and auto-tune it for you. It will let you start training on your local machine, and then scale out to the cloud.
Azure ML Studio	Collaborative visual workspace where you can build, test, and deploy machine learning solutions by using prebuilt machine learning algorithms and data-handling modules.

TABLE 8

A closely related set of products are the *cognitive services*. You can use these prebuilt APIs in your applications to solve complex problems.

Service name	Description
Vision	Use image-processing algorithms to smartly identify, caption, index, and moderate your pictures and videos.
Speech	Convert spoken audio into text, use voice for verification, or add speaker recognition to your app.
Knowledge mapping	Map complex information and data to solve tasks such as intelligent recommendations and semantic search.

Bing Search	Add Bing Search APIs to your apps and harness the ability to comb billions of webpages, images, videos, and news with a single API call.
Natural Language processing	Allow your apps to process natural language with prebuilt scripts, evaluate sentiment, and learn how to recognize what users want.

TABLE 9

DevOps

DevOps brings together people, processes, and technology by automating software delivery to provide continuous value to your users. With Azure DevOps, you can create *build* and *release* pipelines that provide continuous integration, delivery, and deployment for your applications. You can integrate repositories and application tests, perform application monitoring, and work with build artifacts. You can also work with and backlog items for tracking, automate infrastructure deployment, and integrate a range of third-party tools and services such as Jenkins and Chef. All of these functions and many more are closely integrated with Azure to allow for consistent, repeatable deployments for your applications to provide streamlined build and release processes.

Service name	**Description**
Azure DevOps	Use development collaboration tools such as high-performance pipelines, free private Git repositories, configurable Kanban boards, and extensive automated and cloud-based load testing. Formerly known as Visual Studio Team Services.
Azure DevTest Labs	Quickly create on-demand Windows and Linux environments to test or demo applications directly from deployment pipelines.

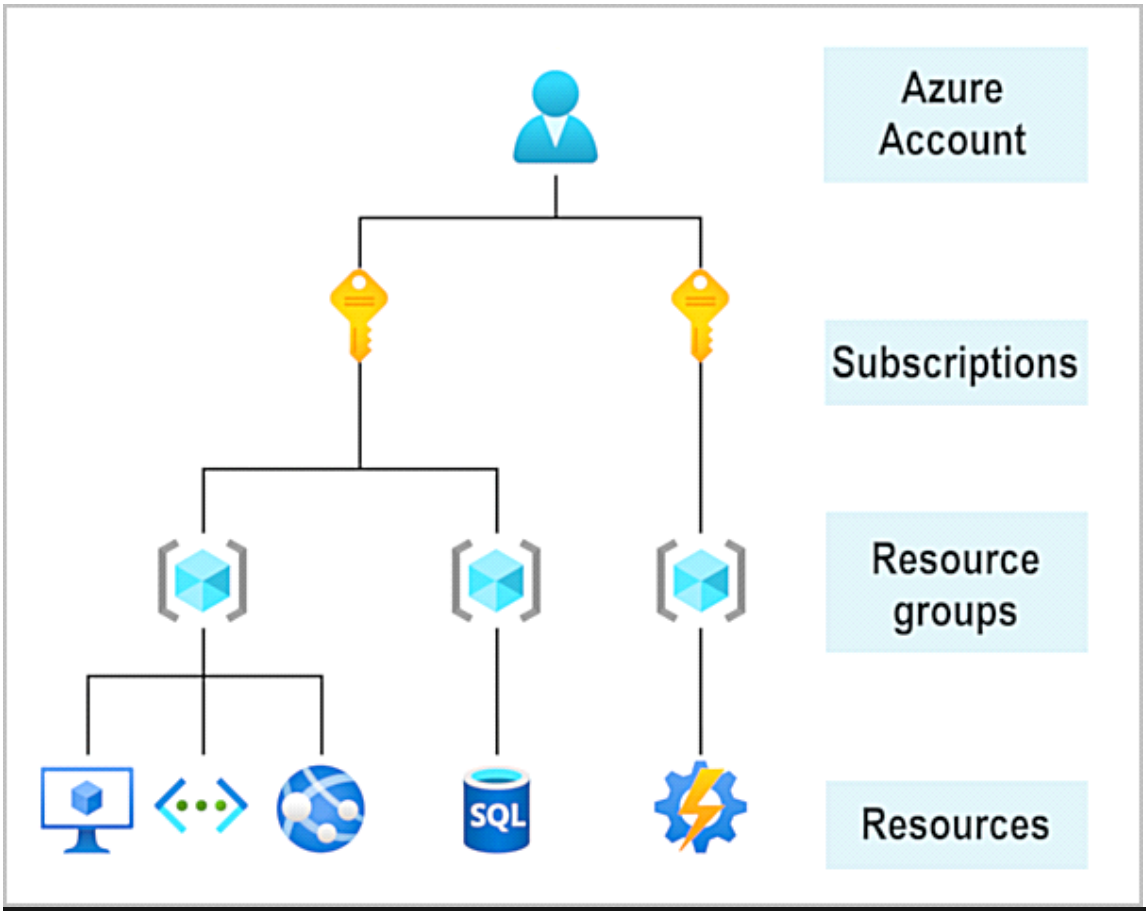
TABLE 10

From <https://docs.microsoft.com/en-us/learn/modules/intro-to-azure-fundamentals/tour-of-azure-services>

Get started with Azure accounts

- 2 minutes

To create and use Azure services, you need an Azure subscription. When you're completing Learn modules, most of the time a temporary subscription is created for you, which runs in an environment called the Learn sandbox. When you're working with your own applications and business needs, you need to create an Azure account, and a subscription will be created for you. After you've created an Azure account, you're free to create additional subscriptions. For example, your company might use a single Azure account for your business and separate subscriptions for development, marketing, and sales departments. After you've created an Azure subscription, you can start creating Azure resources within each subscription.



If you're new to Azure, you can sign up for a free account on the Azure website to start exploring at no cost to you. When you're ready, you can choose to upgrade your free account. You can create a new subscription that enables you to start paying for Azure services you need to use that are beyond the limits of a free account.

Create an Azure account

You can purchase Azure access directly from Microsoft by signing up on the Azure website or through a Microsoft representative. You can also purchase Azure access through a Microsoft partner. Cloud Solution Provider partners offer a range of complete managed-cloud solutions for Azure.
For more information on how to create an Azure account, see the Create an Azure account learning module.

What is the Azure free account?

The Azure free account includes:

- Free access to popular Azure products for 12 months.
- A credit to spend for the first 30 days.
- Access to more than 25 products that are always free.

The Azure free account is an excellent way for new users to get started and explore. To sign up, you need a phone number, a credit card, and a Microsoft or GitHub account. The credit card information is used for identity verification only. You won't be charged

for any services until you upgrade to a paid subscription.

What is the Learn sandbox?

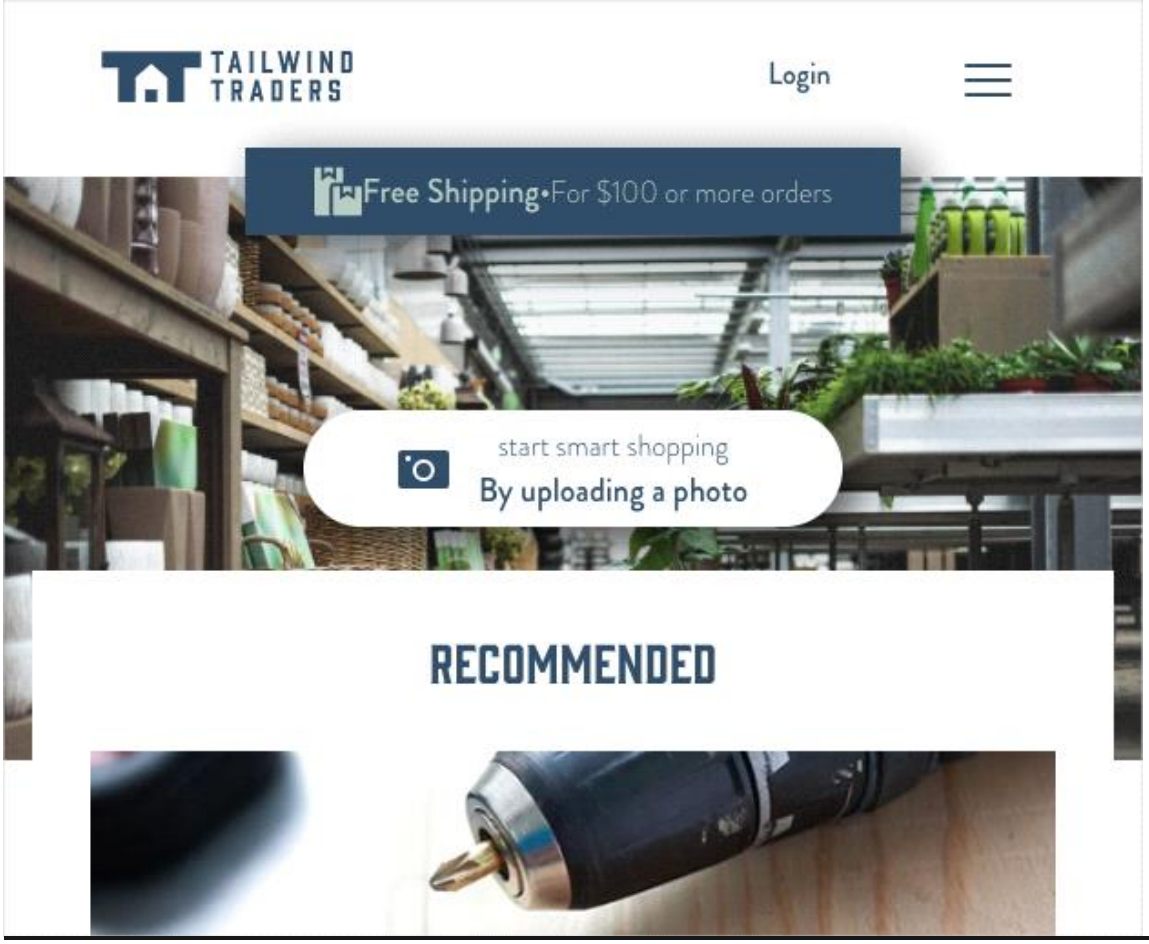
Many of the Learn exercises use a technology called the sandbox, which creates a temporary subscription that's added to your Azure account. This temporary subscription allows you to create Azure resources for the duration of a Learn module. Learn automatically cleans up the temporary resources for you after you've completed the module.
When you're completing a Learn module, you're welcome to use your personal subscription to complete the exercises in a module. The sandbox is the preferred method to use though, because it allows you to create and test Azure resources at no cost to you.

From <https://docs.microsoft.com/en-us/learn/modules/intro-to-azure-fundamentals/get-started-with-azure-accounts>

Case study introduction

- 2 minutes

Throughout the Azure Fundamentals learning paths, we'll work with Tailwind Traders , a fictitious home improvement retailer. It operates retail hardware stores across the globe and online.



Tailwind Traders currently manages an on-premises datacenter that hosts the company's retail website. The datacenter also stores all of the data and streaming video for its applications. The IT department is currently responsible for all of the management tasks for its computing hardware and software. For example, let's suppose that you work as an IT specialist for the company's IT department. Your IT team handles the procurement process to buy new hardware, installs and configures software, and deploys everything throughout the datacenter.

These management responsibilities create some obstacles for delivering your applications to your users in a timely fashion. As an IT pro, you realize it would be advantageous to have servers, storage, databases, and other services immediately available when you develop and deploy applications. You want to easily start a new server or add services to your solutions.

In the other units of this learning module, you've learned about some of the cloud-based services that Tailwind Traders can use to address its technology challenges. With that in mind, the services that are available through Azure can help Tailwind Traders conduct its business more efficiently.

As you complete the various modules in the Azure Fundamentals learning paths, we'll analyze the challenges that Tailwind Traders is facing. You'll see how you can use Azure services to address each of the issues as they arise. After you've completed each of the modules, the knowledge that you gained from resolving the hypothetical challenges that the fictional Tailwind Traders company encountered should benefit you in your real-world environments.

From <https://docs.microsoft.com/en-us/learn/modules/intro-to-azure-fundamentals/case-study-introduction>

Discuss Azure fundamental concepts

Thursday, January 28, 2021 10:15 AM

Are you interested in the cloud, but aren't sure what it can do for you? In this module, you'll learn about the advantages of using cloud computing services, and you'll learn to differentiate between the categories and types of cloud computing.

Overview

- Introduction 2 min
- Describe the benefits of cloud computing 5 min
- Describe the different categories of cloud services 5 min
- Describe the different types of cloud computing 5 min
- Knowledge check 5 min
- Summary 2 min

From <https://docs.microsoft.com/en-us/learn/paths/az-900-describe-cloud-concepts/>

Introduction

- 2 minutes

You work in the IT department for Tailwind Traders, which has decided to migrate its applications and data to Microsoft Azure. You're aware that cloud computing will save your company time and money by migrating from your existing, on-premises, physical hardware, to a cloud solution. With this new solution, you'll only need to pay for the resources and computing time that you use.

However, some of the cloud computing concepts are new to many members of your IT staff. They've been asking some specific questions about what cloud computing can do for them. For example, the team that manages Tailwind Traders' website wants to know how Azure improves the site's availability and scalability. The team that handles the deployment of new hardware is curious to see how cloud computing can make their deployment processes faster.

In addition, your developer team wants to learn about the different options available to them as they are designing new applications. For example, is there a way to run their applications in a hybrid configuration, where part of their application runs on-premises and the rest of the application runs in the cloud?

In this module, you'll learn about the fundamental concepts of cloud computing, how Azure implements these concepts, and how Tailwind Traders might benefit from

migrating to a cloud computing environment.

Learning objectives

Upon completion of this module, you'll be able to:

- Identify the benefits and considerations of using cloud services.
- Describe the differences between categories of cloud services.
- Describe the differences between types of cloud computing.

Prerequisites

- You should be familiar with basic computing concepts and terminology.

From <https://docs.microsoft.com/en-us/learn/modules/fundamental-azure-concepts/introduction>

Describe the benefits of cloud computing

- 5 minutes

What are some cloud computing advantages?

There are several advantages that a cloud environment has over a physical environment that Tailwind Traders can use following its migration to Azure.

- High availability: Depending on the service-level agreement (SLA) that you choose, your cloud-based apps can provide a continuous user experience with no apparent downtime, even when things go wrong.
- Scalability: Apps in the cloud can scale *vertically* and *horizontally*:
- Scale vertically to increase compute capacity by adding RAM or CPUs to a virtual machine.
- Scaling horizontally increases compute capacity by adding instances of resources, such as adding VMs to the configuration.
- Elasticity: You can configure cloud-based apps to take advantage of autoscaling, so your apps always have the resources they need.
- Agility: Deploy and configure cloud-based resources quickly as your app requirements change.
- Geo-distribution: You can deploy apps and data to regional datacenters around the globe, thereby ensuring that your customers always have the best performance in their region.
- Disaster recovery: By taking advantage of cloud-based backup services, data replication, and geo-distribution, you can deploy your apps with the confidence that comes from knowing that your data is safe in the event of disaster.

Cloud computing is a consumption-based model

Cloud service providers operate on a *consumption-based model*, which means that end users only pay for the resources that they use. Whatever they use is what they pay for. A consumption-based model has many benefits, including:

- No upfront costs.
- No need to purchase and manage costly infrastructure that users might not use to its fullest.
- The ability to pay for additional resources when they are needed.
- The ability to stop paying for resources that are no longer needed.

Capital expenses vs. operating expenses

There are two different types of expenses that you should consider:

- Capital Expenditure (CapEx) is the up-front spending of money on physical infrastructure, and then deducting that up-front expense over time. The up-front cost from CapEx has a value that reduces over time.
- Operational Expenditure (OpEx) is spending money on services or products now, and being billed for them now. You can deduct this expense in the same year you spend it. There is no up-front cost, as you pay for a service or product as you use it.

In other words, when Tailwind Traders owns its infrastructure, it buys equipment that goes onto its balance sheets as assets. Because a capital investment was made, accountants categorize this transaction as a CapEx. Over time, to account for the assets' limited useful lifespan, assets are depreciated or amortized.

Cloud services, on the other hand, are categorized as an OpEx, because of their consumption model. There's no asset for Tailwind Traders to amortize, and its cloud service provider (Azure) manages the costs that are associated with the purchase and lifespan of the physical equipment. As a result, OpEx has a direct impact on net profit, taxable income, and the associated expenses on the balance sheet.

To summarize, CapEx requires significant up-front financial costs, as well as ongoing maintenance and support expenditures. By contrast, OpEx is a consumption-based model, so Tailwind Traders is only responsible for the cost of the computing resources that it uses.

From <https://docs.microsoft.com/en-us/learn/modules/fundamental-azure-concepts/benefits-of-cloud-computing>

Describe the different categories of cloud services

- 5 minutes

What are cloud service models?

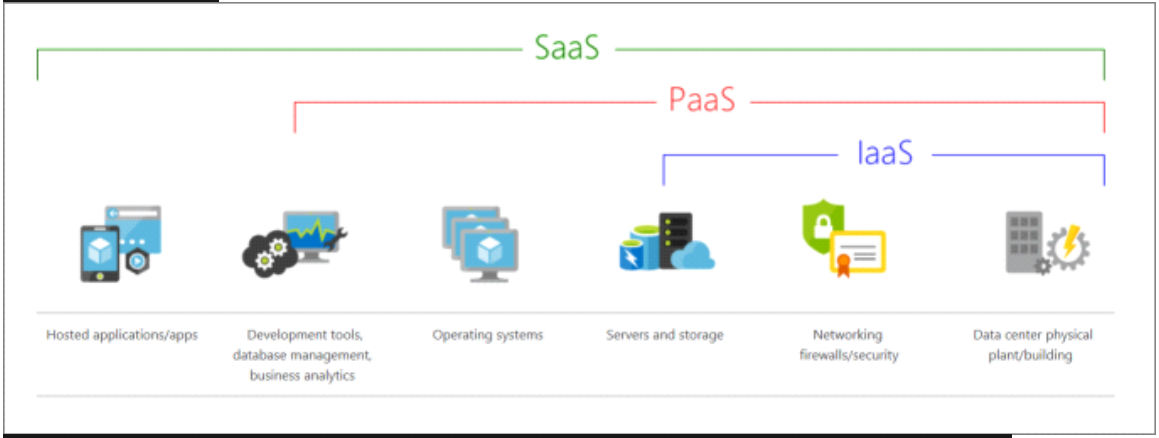
If you've been around cloud computing for a while, you've probably seen the *PaaS*, *IaaS*,

and *SaaS* acronyms for the different *cloud service models*. These models define the different levels of shared responsibility that a cloud provider and cloud tenant are responsible for.

Model	Definition	Description
IaaS	*Infrastructure-as-a-Service*	This cloud service model is the closest to managing physical servers; a cloud provider will keep the hardware up-to-date, but operating system maintenance and network configuration is up to you as the cloud tenant. For example, Azure virtual machines are fully operational virtual compute devices running in Microsoft datacenters. An advantage of this cloud service model is rapid deployment of new compute devices. Setting up a new virtual machine is considerably faster than procuring, installing, and configuring a physical server.
PaaS	*Platform-as-a-Service*	This cloud service model is a managed hosting environment. The cloud provider manages the virtual machines and networking resources, and the cloud tenant deploys their applications into the managed hosting environment. For example, Azure App Services provides a managed hosting environment where developers can upload their web applications, without having to worry about the physical hardware and software requirements.
SaaS	*Software-as-a-Service*	In this cloud service model, the cloud provider manages all aspects of the application environment, such as virtual machines, networking resources, data storage, and applications. The cloud tenant only needs to provide their data to the application managed by the cloud provider. For example, Microsoft Office 365 provides a fully working version of Microsoft Office that runs in the cloud. All you need to do is create your content, and Office 365 takes care of everything else.

WHAT ARE CLOUD SERVICE MODELS?

The following illustration demonstrates the services that might run in each of the cloud service models.



Let's compare the three models in more detail in the following sections.

IaaS

IaaS is the most flexible category of cloud services. It aims to give you complete control over the hardware that runs your application. Instead of buying hardware, with IaaS, you rent it.

Advantages

No CapEx. Users have no up-front costs.
Agility. Applications can be made accessible quickly, and deprovisioned whenever needed.
Management. The shared responsibility model applies; the user manages and maintains the services they have provisioned, and the cloud provider manages and maintains the cloud infrastructure.
Consumption-based model. Organizations pay only for what they use and operate under an Operational Expenditure (OpEx) model.
Skills. No deep technical skills are required to deploy, use, and gain the benefits of a public cloud. Organizations can use the skills and expertise of the cloud provider to ensure workloads are secure, safe, and highly available.
Cloud benefits. Organizations can use the skills and expertise of the cloud provider to ensure workloads are made secure and highly available.
Flexibility. IaaS is the most flexible cloud service because you have control to configure and manage the hardware running your application.

PaaS

PaaS provides the same benefits and considerations as IaaS, but there are some additional benefits to be aware of.

Advantages

No CapEx. Users have no up-front costs.
Agility. PaaS is more agile than IaaS, and users don't need to configure servers for running applications.
Consumption-based model. Users pay only for what they use, and operate under an OpEx model.
Skills. No deep technical skills are required to deploy, use, and gain the benefits of PaaS.
Cloud benefits. Users can take advantage of the skills and expertise of the cloud provider to ensure that their workloads are made secure and highly available. In addition, users can gain access to more cutting-edge development tools. They can then apply these tools across an application's lifecycle.
Productivity. Users can focus on application development only, because the cloud provider handles all platform management. Working with distributed teams as services is easier because the platform is accessed over the internet. You can make the platform available globally more easily.

Disadvantage

Platform limitations. There can be some limitations to a cloud platform that might affect how an application runs. When you're evaluating which PaaS platform is best suited for a workload, be sure to consider any limitations in this area.

SaaS

SaaS is software that's centrally hosted and managed for you and your users or customers. Usually one version of the application is used for all customers, and it's licensed through a monthly or annual subscription.
SaaS provides the same benefits as IaaS, but again there are some additional benefits to be aware of too.

Advantages

No CapEx. Users have no up-front costs.
Agility. Users can provide staff with access to the latest software quickly and easily.
Pay-as-you-go pricing model. Users pay for the software they use on a subscription model, typically monthly or yearly, regardless of how much they use the software.
Skills. No deep technical skills are required to deploy, use, and gain the benefits of SaaS.
Flexibility. Users can access the same application data from anywhere.

Disadvantage

Software limitations. There can be some limitations to a software application that might affect how users work. Because you're using as-is software, you don't have direct control of features. When you're evaluating which SaaS platform is best suited for a workload, be sure to consider any business needs and software limitations.

What is serverless computing?

Like PaaS, *serverless computing* enables developers to build applications faster by eliminating the need for them to manage infrastructure. With serverless applications, the cloud service provider automatically provisions, scales, and manages the infrastructure required to run the code. Serverless architectures are highly scalable and event-driven, only using resources when a specific function or trigger occurs.
It's important to note that servers are still running the code. The "serverless" name comes from the fact that the tasks associated with infrastructure provisioning and management are invisible to the developer. This approach enables developers to increase their focus on the business logic, and deliver more value to the core of the business. Serverless computing helps teams increase their productivity and bring products to market faster, and it allows organizations to better optimize resources and stay focused on innovation.

From <https://docs.microsoft.com/en-us/learn/modules/fundamental-azure-concepts/categories-of-cloud-services>

Describe the different types of cloud computing

- 5 minutes

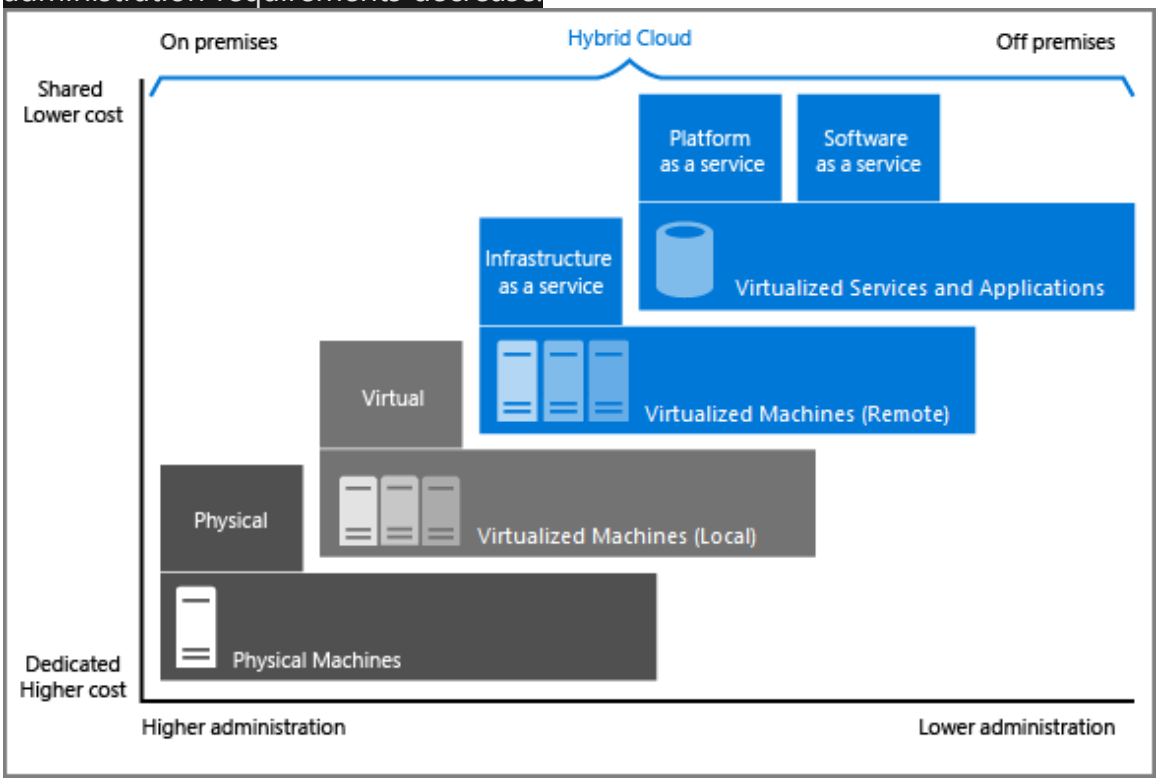
What are public, private, and hybrid clouds?

There are three deployment models for cloud computing: *public cloud*, *private cloud*, and *hybrid cloud*. Each deployment model has different aspects that you should consider as you migrate to the cloud.

Deployment model	Description
Public cloud	Services are offered over the public internet and available to anyone who wants to purchase them. Cloud resources, such as servers and storage, are owned and operated by a third-party cloud service provider, and delivered over the internet.
Private cloud	A private cloud consists of computing resources used exclusively by users from one business or organization. A private cloud can be physically located at your organization's on-site (on-premises) datacenter, or it can be hosted by a third-party service provider.
Hybrid cloud	A hybrid cloud is a computing environment that combines a public cloud and a private cloud by allowing data and applications to be shared between them.

WHAT ARE PUBLIC, PRIVATE, AND HYBRID CLOUDS?

The following image illustrates several of the cloud computing concepts that are presented in this unit. In this example, several factors are demonstrated when you are considering where to deploy a database server in a hybrid cloud environment: as your resources move from on-premises to off-premises, your costs are reduced, and your administration requirements decrease.



From <https://docs.microsoft.com/en-us/learn/modules/fundamental-azure-concepts/types-of-cloud-computing>

Describe core Azure architectural components

Thursday, January 28, 2021 10:16 AM

In this module, you'll examine the various concepts, resources, and terminology that are necessary to work with Azure architecture. For example, you'll learn about Azure subscriptions and management groups, resource groups and Azure Resource Manager, as well as Azure regions and availability zones.

Overview

- Introduction 2 min
- Overview of Azure subscriptions, management groups, resources, and regions 2 min
- Azure subscriptions and management groups 6 min
- Azure resources and Azure Resource Manager 4 min
- Azure regions and availability zones 7 min
- Exercise - Create a website hosted in Azure 7 min
- Knowledge check 4 min
- Summary 2 min

From <https://docs.microsoft.com/en-us/learn/paths/az-900-describe-cloud-concepts/>

Introduction

- 2 minutes

Let's say that you work as a developer for a successful hardware manufacturing company, Tailwind Traders. Your company's Chief Technology Officer recently decided to adopt Azure as the cloud computing platform. You're currently in the planning stages for the migration. Before you begin the migration process, you decide to study Azure concepts, resources, and terminology to ensure your migration is a success.

In this module, you'll learn about several of the components that are necessary to successfully deploy resources on Azure.

Learning objectives

After completing this module, you'll be able to describe the benefits and usage of:

- Azure subscriptions and management groups.

- Azure resources, resource groups, and Azure Resource Manager.
- Azure regions, region pairs, and availability zones.

Prerequisites

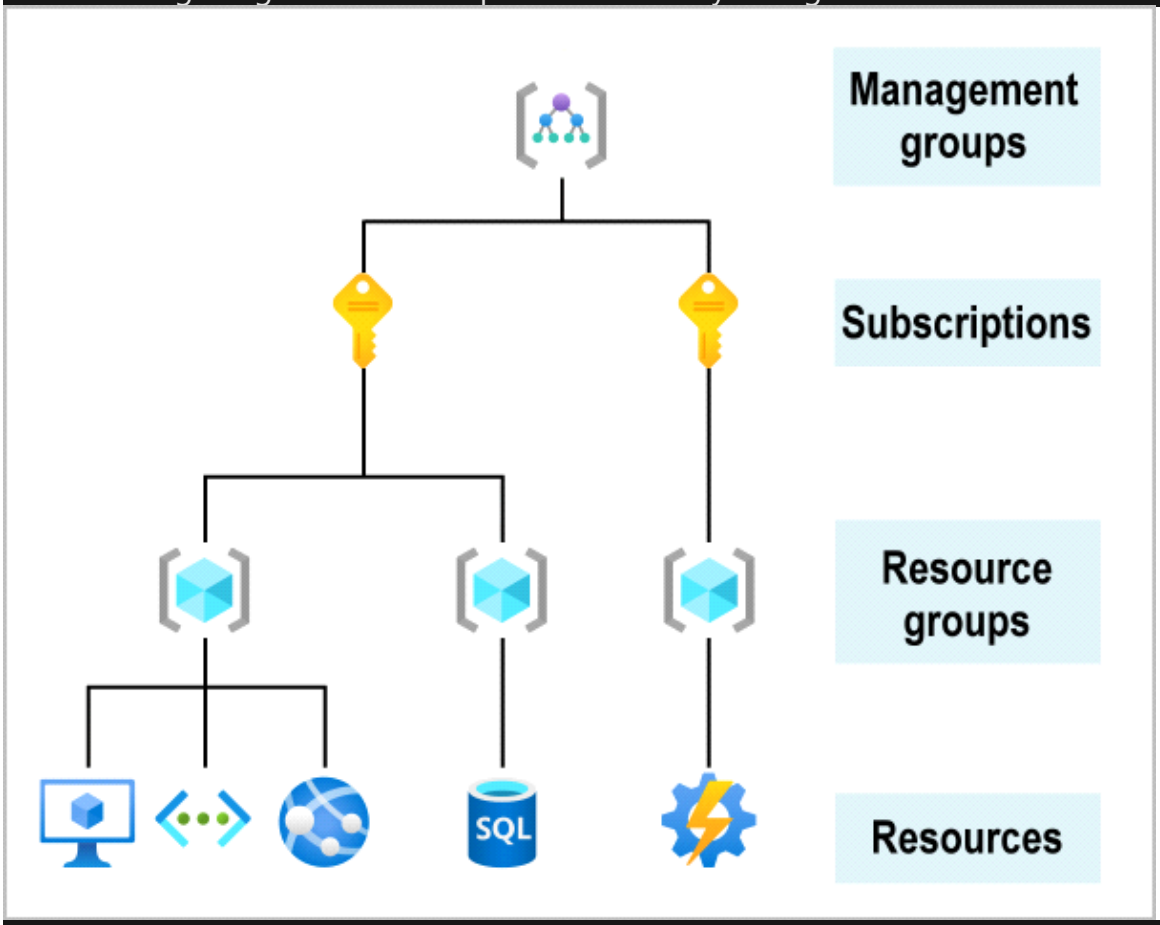
- You should be familiar with basic computing concepts and terminology.
- Familiarity with cloud computing is helpful but isn't necessary.

From <https://docs.microsoft.com/en-us/learn/modules/azure-architecture-fundamentals/introduction>

Overview of Azure subscriptions, management groups, resources, and regions

- 2 minutes

As part of your research for Tailwind Traders, you need to learn the organizing structure for resources in Azure, which has four levels: management groups, subscriptions, resource groups, and resources.
The following image shows the top-down hierarchy of organization for these levels.



Having seen the top-down hierarchy of organization, let's describe each of those levels from the bottom up:

- Resources: Resources are instances of services that you create, like virtual machines, storage, or SQL databases.

- Resource groups: Resources are combined into resource groups, which act as a logical container into which Azure resources like web apps, databases, and storage accounts are deployed and managed.
- Subscriptions: A subscription groups together user accounts and the resources that have been created by those user accounts. For each subscription, there are limits or quotas on the amount of resources that you can create and use. Organizations can use subscriptions to manage costs and the resources that are created by users, teams, or projects.
- Management groups: These groups 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.

You'll examine each of these four organizational levels in the next few units.

From <https://docs.microsoft.com/en-us/learn/modules/azure-architecture-fundamentals/overview>

Azure subscriptions and management groups

- 6 minutes

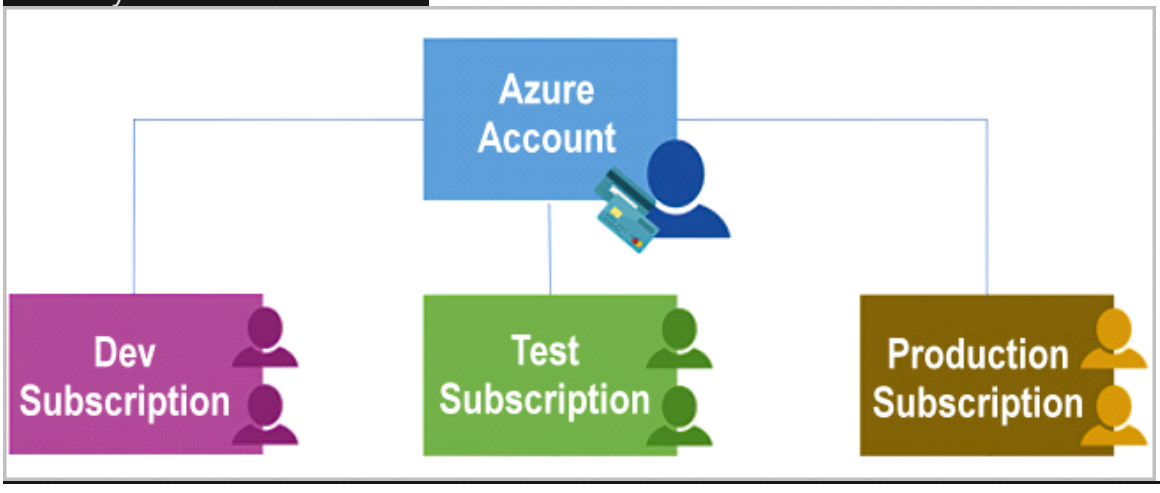
As Tailwind Traders gets started with Azure, one of your first steps will be to create at least one Azure subscription. You'll use it to create your cloud-based resources in Azure.

Note

An Azure resource is a manageable item that's available through Azure. Virtual machines (VMs), storage accounts, web apps, databases, and virtual networks are all examples of resources.

Azure subscriptions

Using Azure requires an Azure subscription. A subscription provides you with authenticated and authorized access to Azure products and services. It also allows you to provision resources. An Azure subscription is a logical unit of Azure services that links to an Azure account, which is an identity in Azure Active Directory (Azure AD) or in a directory that Azure AD trusts.



An account can have one subscription or multiple subscriptions that have different billing models and to which you apply different access-management policies. You can use Azure subscriptions to define boundaries around Azure products, services, and resources. There are two types of subscription boundaries that you can use:

- Billing boundary: This subscription type determines how an Azure account is billed for using Azure. You can create multiple subscriptions for different types of billing requirements. Azure generates separate billing reports and invoices for each subscription so that you can organize and manage costs.
- Access control boundary: Azure applies access-management policies at the subscription level, and you can create separate subscriptions to reflect different organizational structures. An example is that within a business, you have different departments to which you apply distinct Azure subscription policies. This billing model allows you to manage and control access to the resources that users provision with specific subscriptions.

Create additional Azure subscriptions

You might want to create additional subscriptions for resource or billing management purposes. For example, you might choose to create additional subscriptions to separate:

- Environments: When managing your resources, you can choose to create subscriptions to set up separate environments for development and testing, security, or to isolate data for compliance reasons. This design is particularly useful because resource access control occurs at the subscription level.
- Organizational structures: You can create subscriptions to reflect different organizational structures. For example, you could limit a team to lower-cost resources, while allowing the IT department a full range. This design allows you to manage and control access to the resources that users provision within each subscription.
- Billing: You might want to also create additional subscriptions for billing purposes. Because costs are first aggregated at the subscription level, you might want to create subscriptions to manage and track costs based on your needs. For instance, you might want to create one subscription for your production workloads and another subscription for your development and testing workloads.

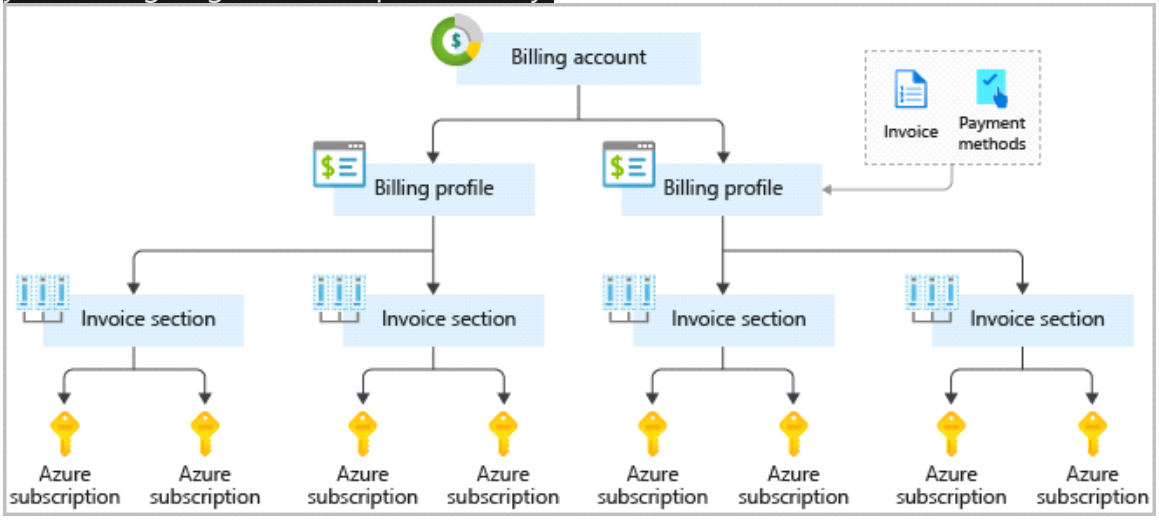
You might also need additional subscriptions because of:

- Subscription limits: Subscriptions are bound to some hard limitations. For example, the maximum number of Azure ExpressRoute circuits per subscription is 10. Those limits should be considered as you create subscriptions on your account. If there's a need to go over those limits in particular scenarios, you might need additional subscriptions.

Customize billing to meet your needs

If you have multiple subscriptions, you can organize them into invoice sections. Each

invoice section is a line item on the invoice that shows the charges incurred that month. For example, you might need a single invoice for your organization but want to organize charges by department, team, or project.
Depending on your needs, you can set up multiple invoices within the same billing account. To do this, create additional billing profiles. Each billing profile has its own monthly invoice and payment method.
The following diagram shows an overview of how billing is structured. If you've previously signed up for Azure or if your organization has an Enterprise Agreement, your billing might be set up differently.



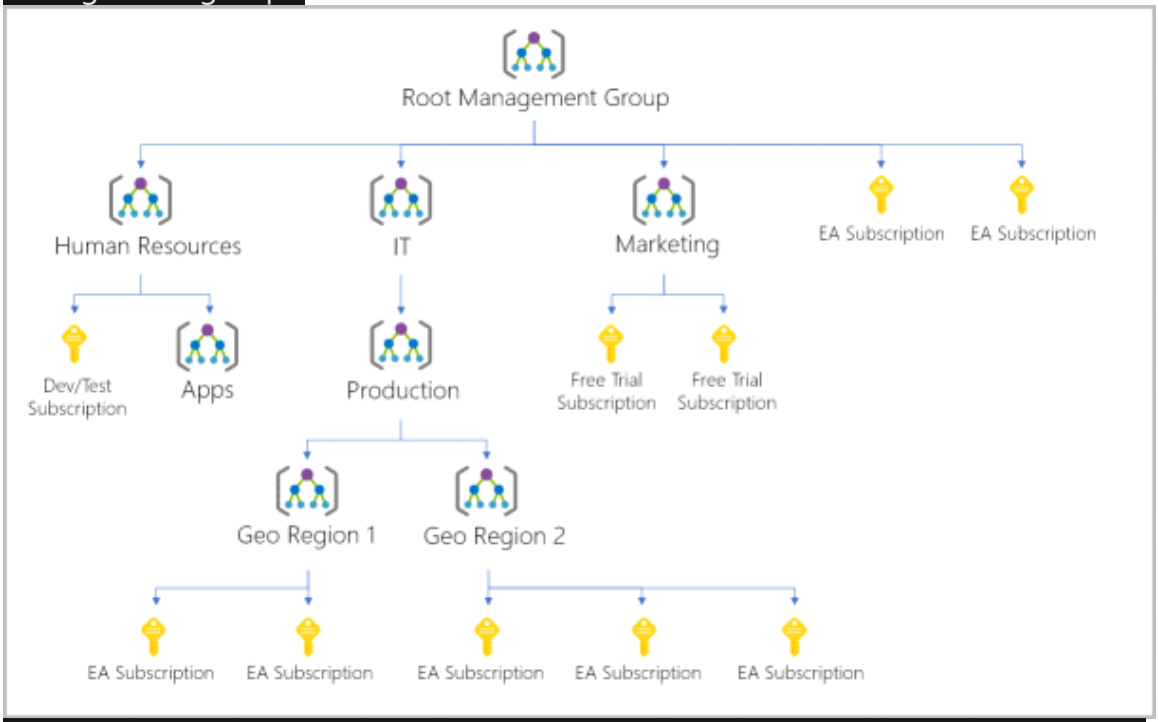
Azure management groups

If your organization has many subscriptions, you might 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 called 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. Management groups give you enterprise-grade management at a large scale no matter what type of subscriptions you might have. All subscriptions within a single management group must trust the same Azure AD tenant.
For example, you can apply policies to a management group that limits the regions available for VM creation. This policy would be applied to all management groups, subscriptions, and resources under that management group by only allowing VMs to be created in that region.

Hierarchy of management groups and subscriptions

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.



You can create a hierarchy that applies a policy. For example, you could limit VM locations to the US West Region in a group called Production. This policy will inherit onto all the Enterprise Agreement subscriptions that are descendants of that management group and will apply to all VMs under those subscriptions. This security policy can't be altered by the resource or subscription owner, which allows for improved governance.

Another scenario where you would use management groups is to provide user access to multiple subscriptions. By moving multiple subscriptions under that management group, you can create one role-based access control (RBAC) assignment on the management group, which will inherit that access to all the subscriptions. One assignment on the management group can enable users to have access to everything they need instead of scripting RBAC over different subscriptions.

Important facts about management groups

- 10,000 management groups can be supported in a single directory.
- A management group tree can support up to six levels of depth. This limit doesn't include the root level or the subscription level.
- Each management group and subscription can support only one parent.
- Each management group can have many children.
- All subscriptions and management groups are within a single hierarchy in each directory.

From <https://docs.microsoft.com/en-us/learn/modules/azure-architecture-fundamentals/management-groups-subscriptions>

Azure resources and Azure Resource Manager

- 4 minutes

After you've created a subscription for Tailwind Traders, you're ready to start creating resources and storing them in resource groups. With that in mind, it's important to define those terms:

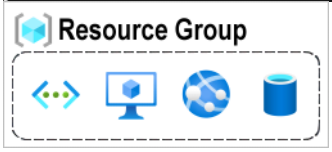
- Resource: A manageable item that's available through Azure. Virtual machines (VMs), storage accounts, web apps, databases, and virtual networks are examples of resources.
- Resource group: A container that holds related resources for an Azure solution. The resource group includes resources that you want to manage as a group. You decide which resources belong in a resource group based on what makes the most sense for your organization.

Azure resource groups

Resource groups are a fundamental element of the Azure platform. A resource group is a logical container for resources deployed on Azure. These resources are anything you create in an Azure subscription like VMs, Azure Application Gateway instances, and Azure Cosmos DB instances. All resources must be in a resource group, and a resource can only be a member of a single resource group. Many resources can be moved between resource groups with some services having specific limitations or requirements to move. Resource groups can't be nested. Before any resource can be provisioned, you need a resource group for it to be placed in.

Logical grouping

Resource groups exist to help manage and organize your Azure resources. By placing resources of similar usage, type, or location in a resource group, you can provide order and organization to resources you create in Azure. Logical grouping is the aspect that you're most interested in here, because there's a lot of disorder among our resources.



Life cycle

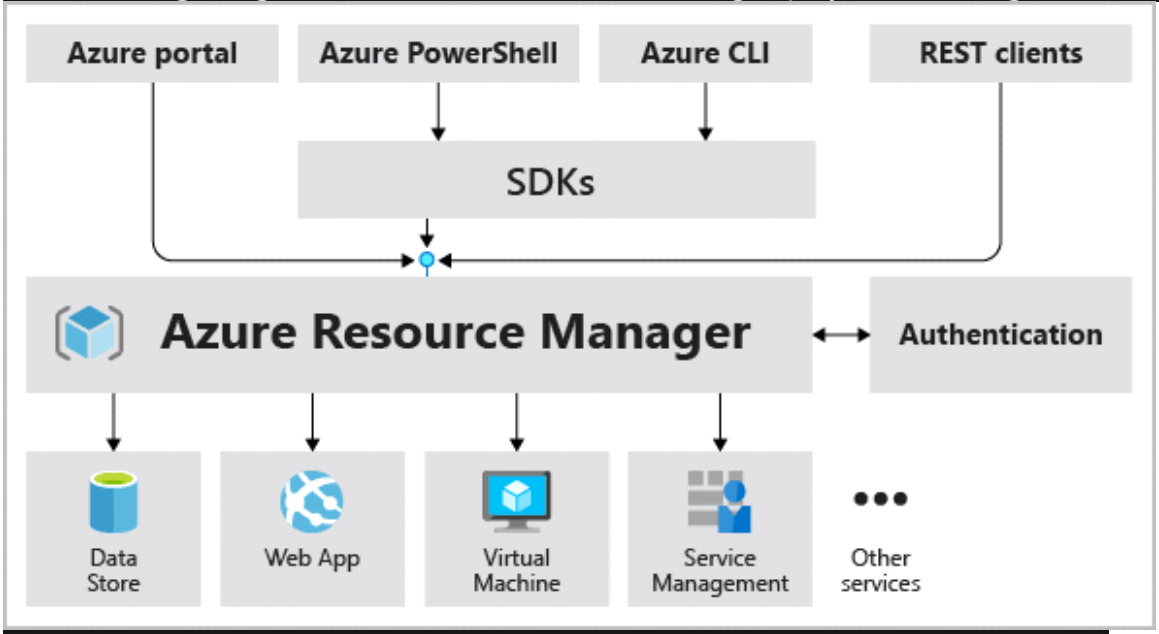
If you delete a resource group, all resources contained within it are also deleted. Organizing resources by life cycle can be useful in nonproduction environments, where you might try an experiment and then dispose of it. Resource groups make it easy to remove a set of resources all at once.

Authorization

Resource groups are also a scope for applying role-based access control (RBAC) permissions. By applying RBAC permissions to a resource group, you can ease administration and limit access to allow only what's needed.

Azure Resource Manager

Azure Resource Manager is the deployment and management service for Azure. It provides a management layer that enables you to create, update, and delete resources in your Azure account. You use management features like access control, locks, and tags to secure and organize your resources after deployment.
When a user sends a request from any of the Azure tools, APIs, or SDKs, Resource Manager receives the request. It authenticates and authorizes the request. Resource Manager sends the request to the Azure service, which takes the requested action. Because all requests are handled through the same API, you see consistent results and capabilities in all the different tools.
The following image shows the role Resource Manager plays in handling Azure requests.



All capabilities that are available in the Azure portal are also available through PowerShell, the Azure CLI, REST APIs, and client SDKs. Functionality initially released through APIs will be represented in the portal within 180 days of initial release.

The benefits of using Resource Manager

With Resource Manager, you can:

- Manage your infrastructure through declarative templates rather than scripts. A Resource Manager template is a JSON file that defines what you want to deploy to Azure.
- Deploy, manage, and monitor all the resources for your solution as a group, rather

than handling these resources individually.
- Redeploy your solution throughout the development life cycle and have confidence your resources are deployed in a consistent state.
- Define the dependencies between resources so they're deployed in the correct order.
- Apply access control to all services because RBAC is natively integrated into the management platform.
- Apply tags to resources to logically organize all the resources in your subscription.
- Clarify your organization's billing by viewing costs for a group of resources that share the same tag.

From <https://docs.microsoft.com/en-us/learn/modules/azure-architecture-fundamentals/resources-resource-manager>

Azure regions and availability zones

- 7 minutes

In the previous unit, you learned about Azure resources and resource groups. Resources are created in regions, which are different geographical locations around the globe that contain Azure datacenters.

Azure is made up of datacenters located around the globe. When you use a service or create a resource such as a SQL database or virtual machine (VM), you're using physical equipment in one or more of these locations. These specific datacenters aren't exposed to users directly. Instead, Azure organizes them into regions. As you'll see later in this unit, some of these regions offer availability zones, which are different Azure datacenters within that region.

Azure regions

A *region* is a geographical area on the planet that contains at least one but potentially multiple datacenters that are nearby and networked together with a low-latency network. Azure intelligently assigns and controls the resources within each region to ensure workloads are appropriately balanced.

When you deploy a resource in Azure, you'll often need to choose the region where you want your resource deployed.

Important

Some services or VM features are only available in certain regions, such as specific VM sizes or storage types. There are also some global Azure services that don't require you to select a particular region, such as Azure Active Directory, Azure Traffic Manager, and Azure DNS.

A few examples of regions are West US, Canada Central, West Europe, Australia East, and Japan West. Here's a view of all the available regions as of June 2020.

Why are regions important?

Azure has more global regions than any other cloud provider. These regions give you the flexibility to bring applications closer to your users no matter where they are. Global regions provide better scalability and redundancy. They also preserve data residency for your services.

Special Azure regions

Azure has specialized regions that you might want to use when you build out your applications for compliance or legal purposes. A few examples include:

- US DoD Central, US Gov Virginia, US Gov Iowa and more: These regions are physical and logical network-isolated instances of Azure for U.S. government agencies and partners. These datacenters are operated by screened U.S. personnel and include additional compliance certifications.
- China East, China North, and more: These regions are available through a unique partnership between Microsoft and 21Vianet, whereby Microsoft doesn't directly maintain the datacenters.

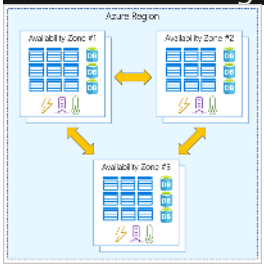
Regions are what you use to identify the location for your resources. There are two other terms you should also be aware of: *geographies* and *availability zones*.

Azure availability zones

You want to ensure your services and data are redundant so you can protect your information in case of failure. When you host your infrastructure, setting up your own redundancy requires that you create duplicate hardware environments. Azure can help make your app highly available through availability zones.

What is an availability zone?

Availability zones are physically separate datacenters within an Azure region. Each availability zone is made up of one or more datacenters equipped with independent power, cooling, and networking. An availability zone is set up to be an *isolation boundary*. If one zone goes down, the other continues working. Availability zones are connected through high-speed, private fiber-optic networks.



Supported regions

Not every region has support for availability zones. For an updated list, see Regions that support availability zones in Azure .

Use availability zones in your apps

You can use availability zones to run mission-critical applications and build high-availability into your application architecture by co-locating your compute, storage, networking, and data resources within a zone and replicating in other zones. Keep in mind that there could be a cost to duplicating your services and transferring data between zones.

Availability zones are primarily for VMs, managed disks, load balancers, and SQL databases. Azure services that support availability zones fall into two categories:

- Zonal services: You pin the resource to a specific zone (for example, VMs, managed disks, IP addresses).
- Zone-redundant services: The platform replicates automatically across zones (for example, zone-redundant storage, SQL Database).

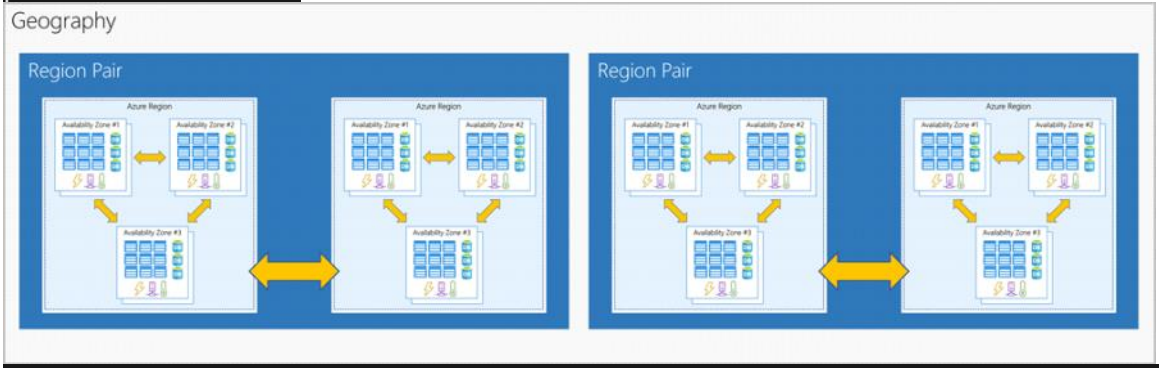
Check the documentation to determine which elements of your architecture you can associate with an availability zone.

Azure region pairs

Availability zones are created by using one or more datacenters. There's a minimum of three zones within a single region. It's possible that a large disaster could cause an outage big enough to affect even two datacenters. That's why Azure also creates *region pairs*.

What is a region pair?

Each Azure region is always paired with another region within the same geography (such as US, Europe, or Asia) at least 300 miles away. This approach allows for the replication of resources (such as VM storage) across a geography that helps reduce the likelihood of interruptions because of events such as natural disasters, civil unrest, power outages, or physical network outages that affect both regions at once. If a region in a pair was affected by a natural disaster, for instance, services would automatically failover to the other region in its region pair.
Examples of region pairs in Azure are West US paired with East US and SouthEast Asia paired with East Asia.



Because the pair of regions is directly connected and far enough apart to be isolated from regional disasters, you can use them to provide reliable services and data redundancy. Some services offer automatic geo-redundant storage by using region pairs.
Additional advantages of region pairs:

- If an extensive Azure outage occurs, one region out of every pair is prioritized to make sure at least one is restored as quickly as possible for applications hosted in that region pair.
- Planned Azure updates are rolled out to paired regions one region at a time to minimize downtime and risk of application outage.
- Data continues to reside within the same geography as its pair (except for Brazil South) for tax- and law-enforcement jurisdiction purposes.

Having a broadly distributed set of datacenters allows Azure to provide a high guarantee of availability.

From <https://docs.microsoft.com/en-us/learn/modules/azure-architecture-fundamentals/regions-availability-zones>

Exercise - Create a website hosted in Azure

- 7 minutes

This module requires a sandbox to complete. A sandbox gives you access to free resources. Your personal subscription will not be charged. The sandbox may only be used to complete training on Microsoft Learn. Use for any other reason is prohibited, and may result in permanent loss of access to the sandbox.

Sign in to activate sandbox

As a developer for Tailwind Traders, you likely have expertise creating applications. As you migrate to Azure, many of the steps that you'll follow to set up a website in the cloud will parallel the steps that you followed when you created websites in your company's datacenter. For example, you need to choose where you'll create your website, and then allocate the necessary resources. In Azure, the physical hardware is managed for you, so your tasks are to choose where your website will be located and which resources to provide.

In this exercise, you'll create an Azure App Service instance to host a WordPress website.

Azure terminology and concepts

Before you get started, let's review and discuss some basic terms and concepts that you'll need to know when you create your website.

What is App Service?

App Service is an HTTP-based service that enables you to build and host many types of web-based solutions without managing infrastructure. For example, you can host web apps, mobile back ends, and RESTful APIs in several supported programming languages. Applications developed in .NET, .NET Core, Java, Ruby, Node.js, PHP, or Python can run in and scale with ease on both Windows- and Linux-based environments.

For this exercise, we want to create a website in less than the time it takes to eat lunch. So, we're not going to write any code. Instead, you'll deploy a predefined application from Azure Marketplace.

What is Azure Marketplace?

Azure Marketplace is an online store that hosts applications that are certified and optimized to run in Azure. Many types of applications are available, ranging from AI and machine learning to web applications. As you'll see in a couple of minutes, deployments from the store are done via the Azure portal by using a wizard-style user interface. This user interface makes evaluating different solutions easy.

We're going to use one of the WordPress application options from Azure Marketplace for our website.

Create resources in Azure

Typically, the first thing we'd do is to create a *resource group* to hold all the things that we need to create. The resource group allows us to administer all the services, disks, network interfaces, and other elements that potentially make up our solution as a unit. We can use the Azure portal to create and manage our solution's resource groups. Keep

in mind that you can also manage resources via a command line by using the Azure CLI. The Azure CLI is a useful option if you need to automate the process in the future. In the free Azure sandbox environment, you'll use the pre-created resource group [sandbox resource group name], and you don't need to do this step.

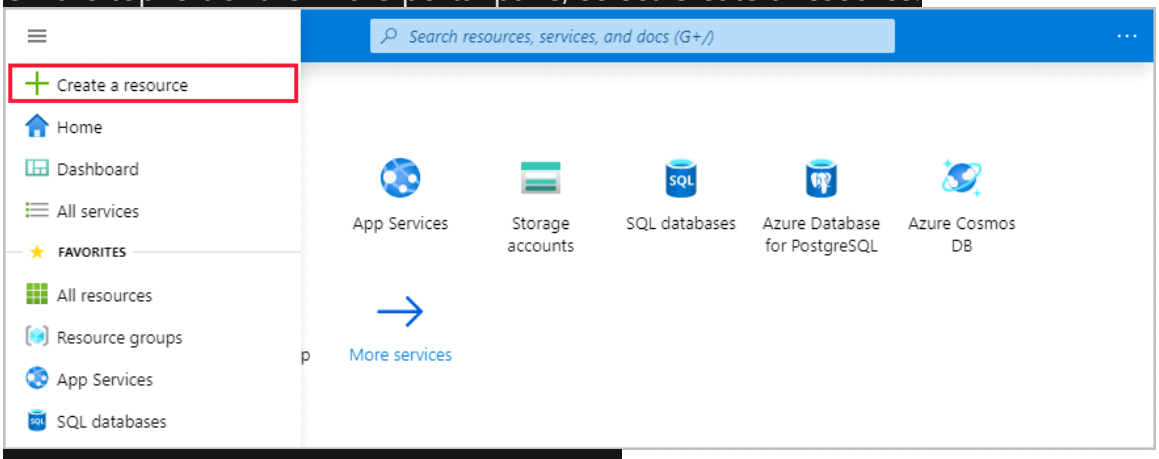
Choose a location

The free sandbox allows you to create resources in a subset of the Azure global regions. Select a region from this list when you create resources:

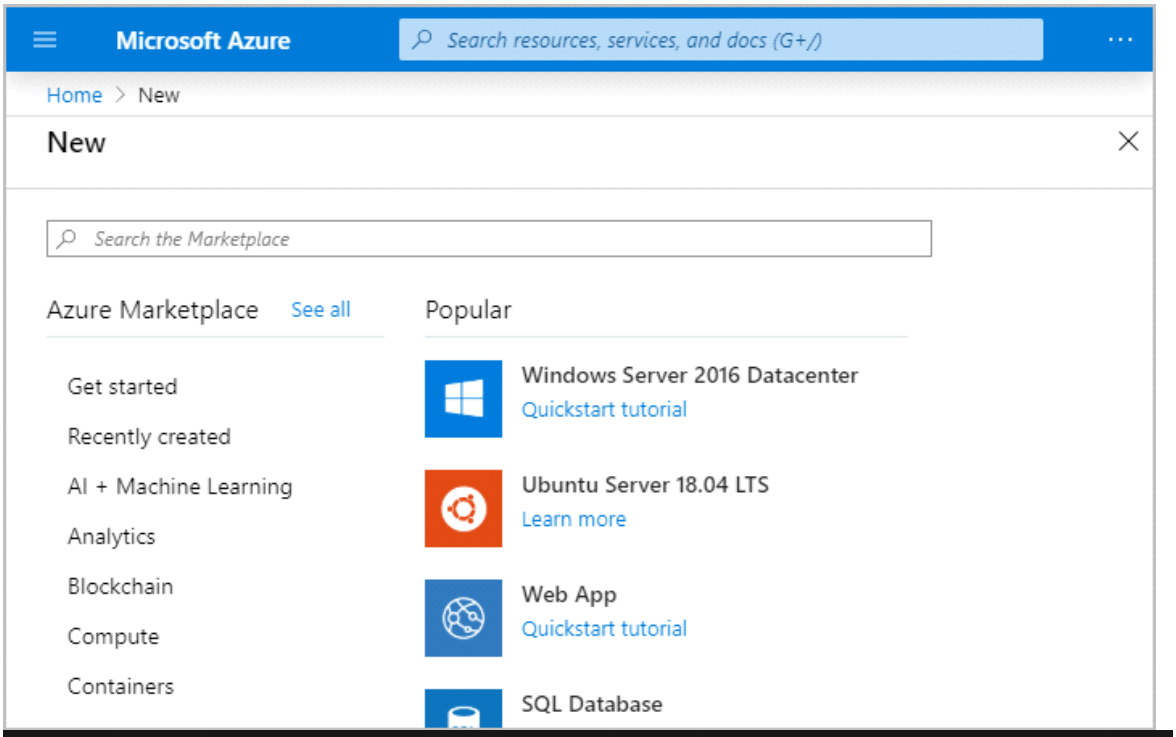
- westus2
- southcentralus
- centralus
- eastus
- westeurope
- southeastasia
- japaneast
- brazilsouth
- australiasoutheast
- centralindia

Create a WordPress website

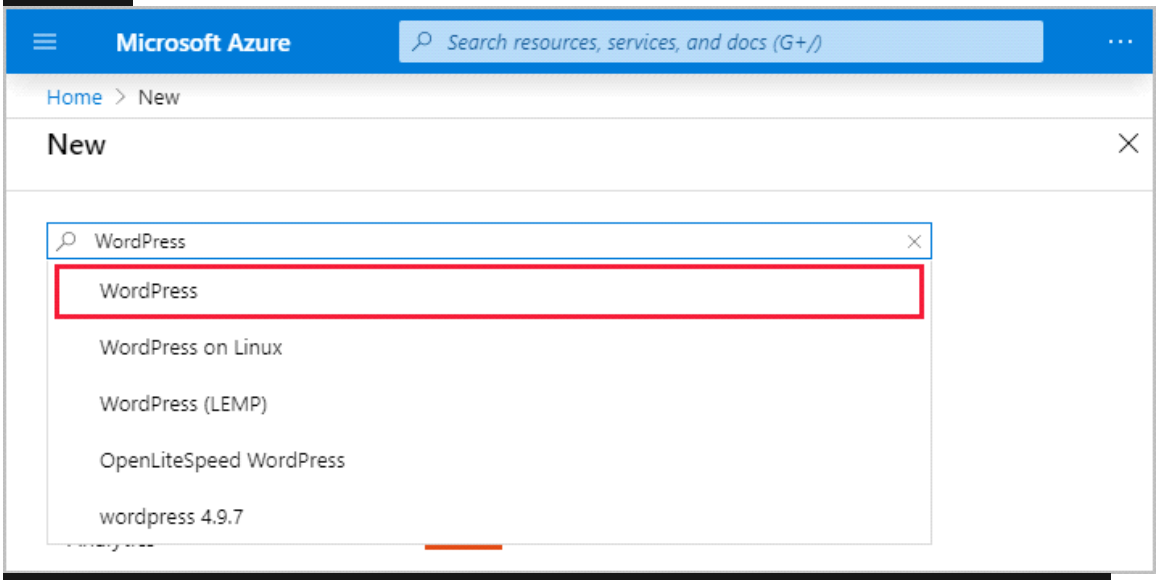
1. If you haven't done so already, verify that you've activated the sandbox. Activating the sandbox allocates the subscription and resource group you'll use in this exercise. This step is required for any Microsoft Learn exercises that use a sandbox.
2. Sign in to the Azure portal by using the same account you used to activate the sandbox.
3. On the top left of the Azure portal pane, select Create a resource.



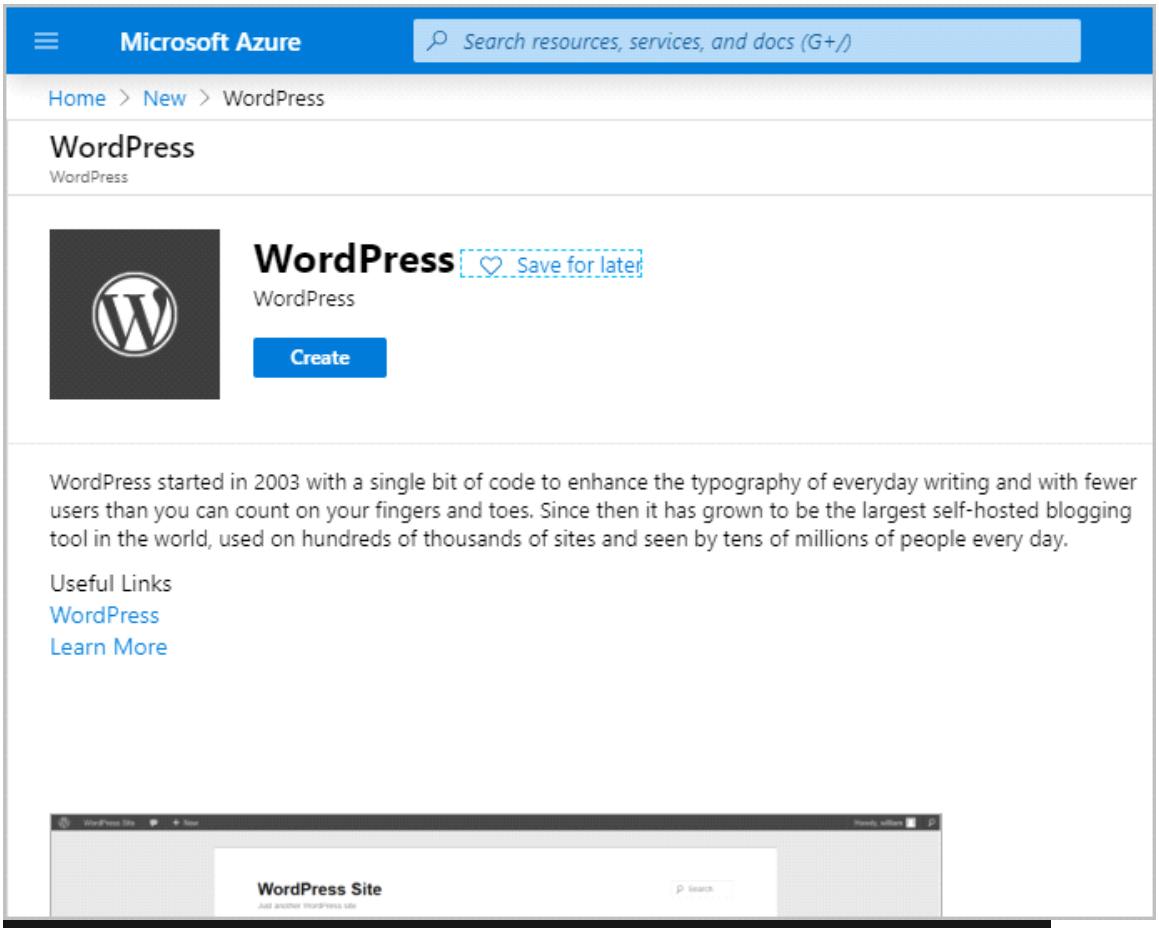
This option takes you to Azure Marketplace.



4. Azure Marketplace has many services, solutions, and resources available for you to use. We know that we want to install WordPress, so we can do a quick search for it. In the Search the Marketplace box with the listed application options, enter WordPress. Select the default WordPress option from the list of options available.



5. In the pane that appears, you'll typically find more information about the item you're about to install, such as the publisher, a brief description of the resource, and links to more information. Make sure to review this information. Select Create to begin the process to create a WordPress app.

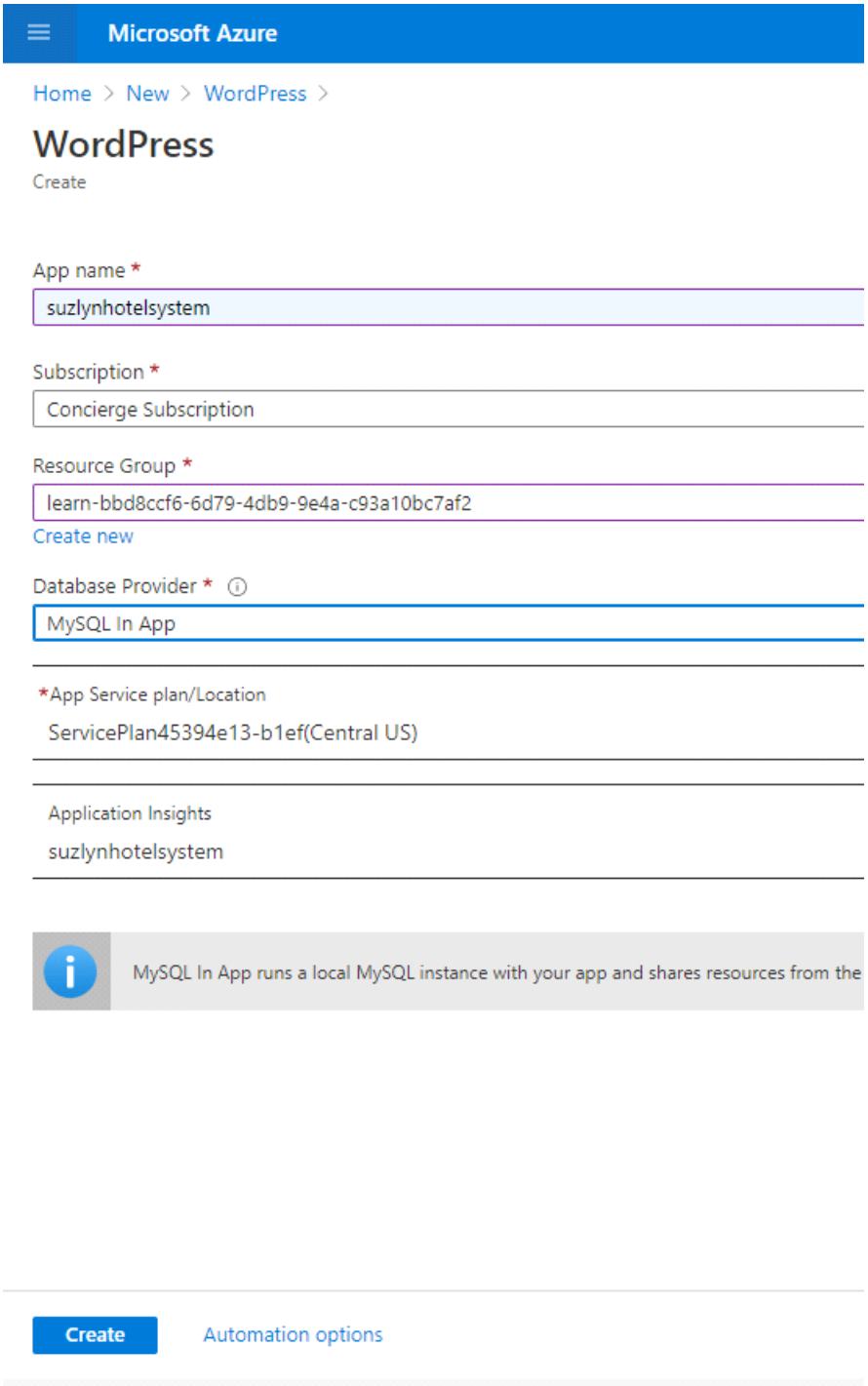


6. Several options to configure your deployment appear. Enter the following information:

Property	Value
App name	Choose a unique value for the app name. It will form part of a fully qualified domain name (FQDN).
Subscription	Make sure Concierge Subscription is selected.
Resource Group	Select the Use existing option, and then select the [sandbox resource group name] resource group from the dropdown.
Database Provider	From the dropdown, select MySQL in App.
App Service plan/Location	You'll change the App Service plan in the next step.
Application Insights	Leave at the default configuration.

TABLE 1

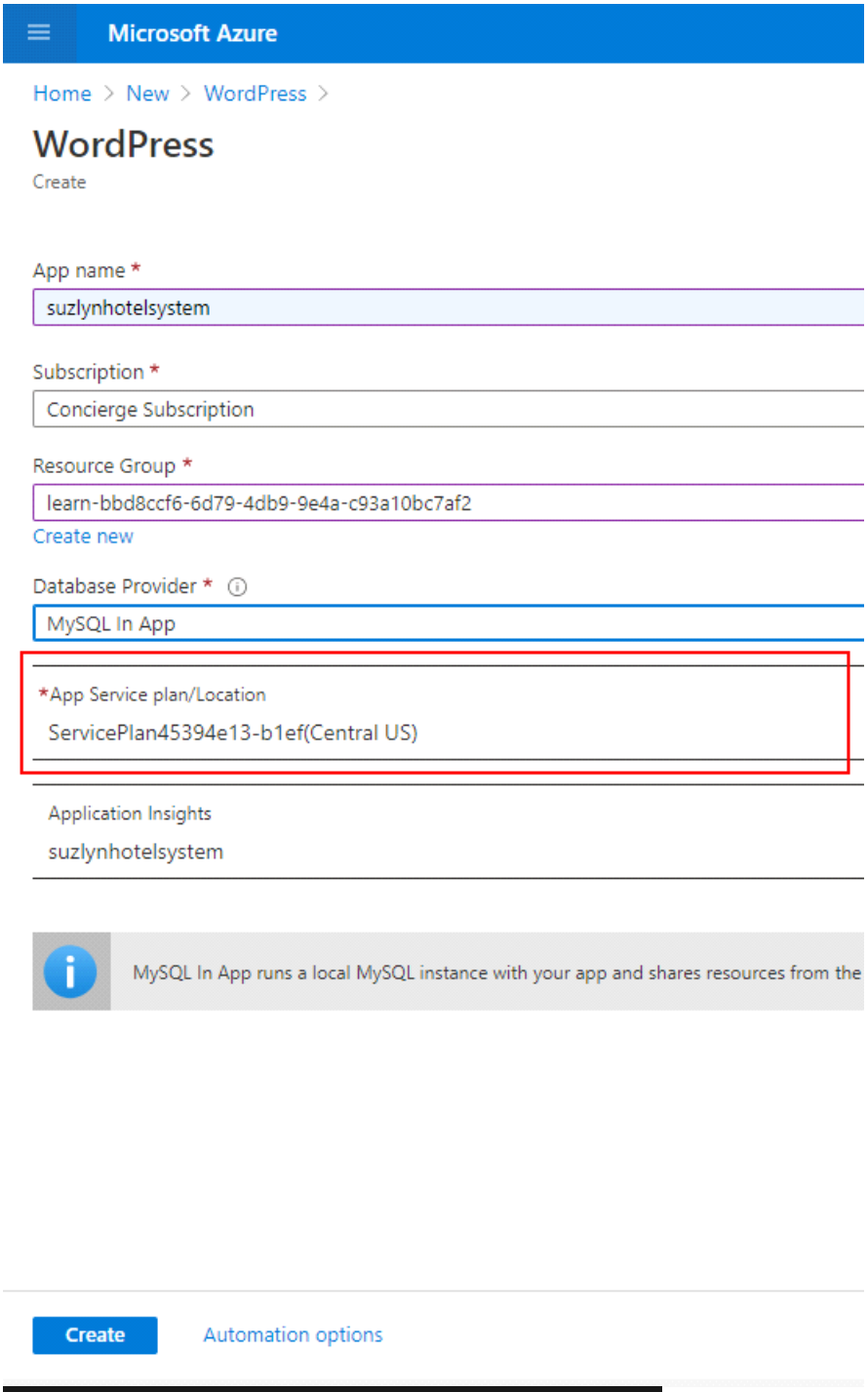
Your configuration should look like this example.



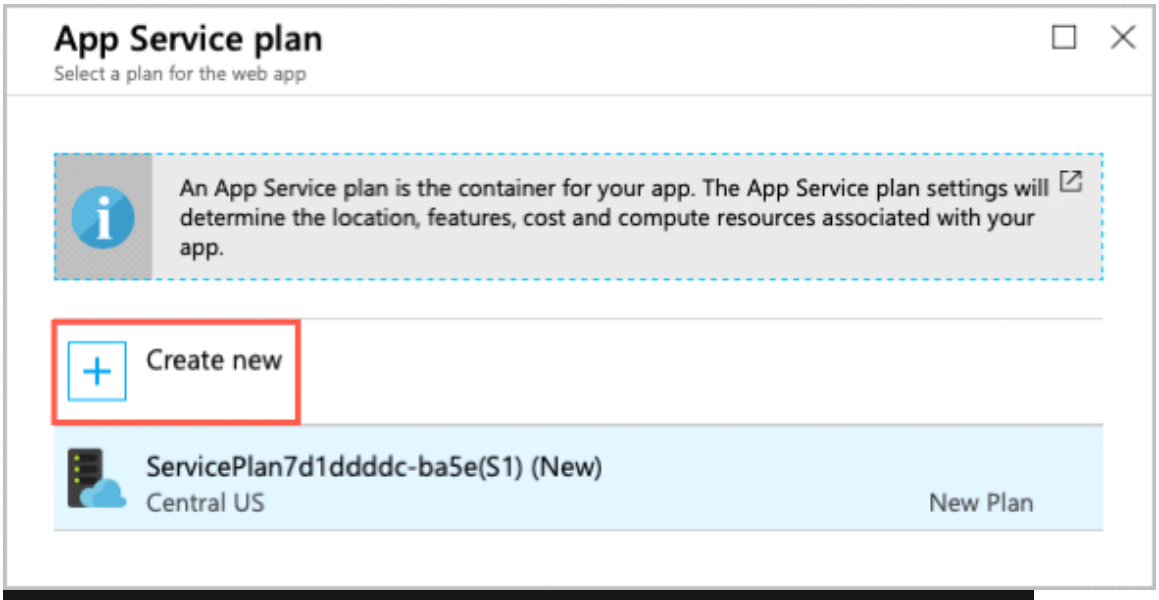
Note

If you still see a section called Database, make sure you selected the correct Database Provider described in the preceding configuration.

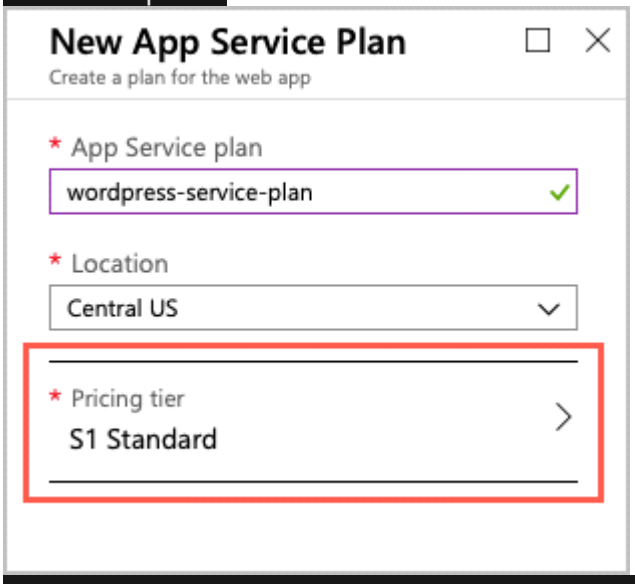
7. Now let's configure the App Service plan to use a specific pricing tier. The App Service plan specifies the compute resources and location for the web app. Select App Service plan/Location.



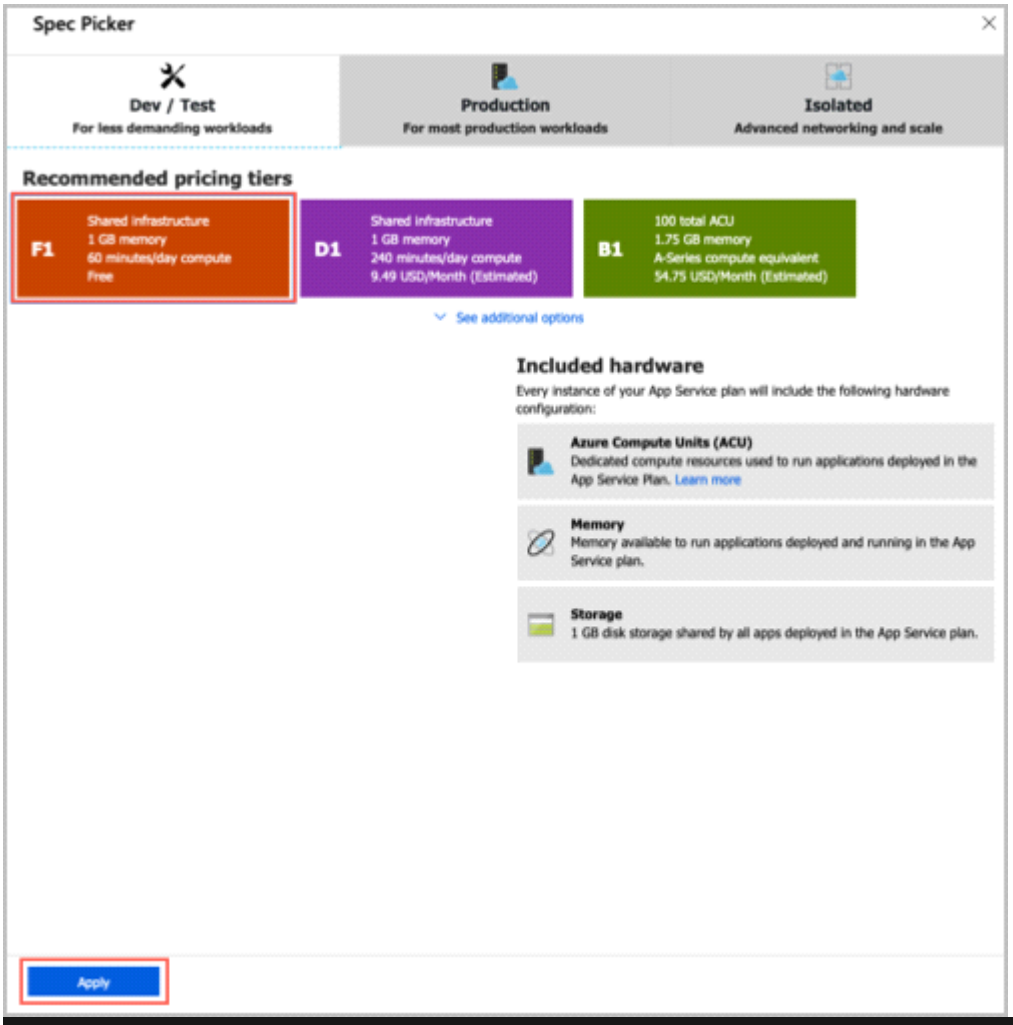
8. In the App Service plan pane, select Create new.



9. In the New App Service plan pane, enter a name for the new service plan.
10. For Location, select Central US to make sure we choose a region that allows the service plan you'll choose. Normally, you'll select the region that's closest to your customers while offering the services you need.
11. Select Pricing tier to see the performance and feature options of the various types of service plans.



12. The Spec Picker enables us to select a new pricing tier for our application. This screen opens to the Production tab, with the S1 pricing tier selected. We'll select a new pricing tier from the Dev / Test tab for our website.
Select the Dev / Test tab, then select the F1 pricing tier, and then select Apply.



13. Back on the New App Service Plan pane, select OK to create the new plan.
14. Finally, select Create to start the deployment of your new site.

Note

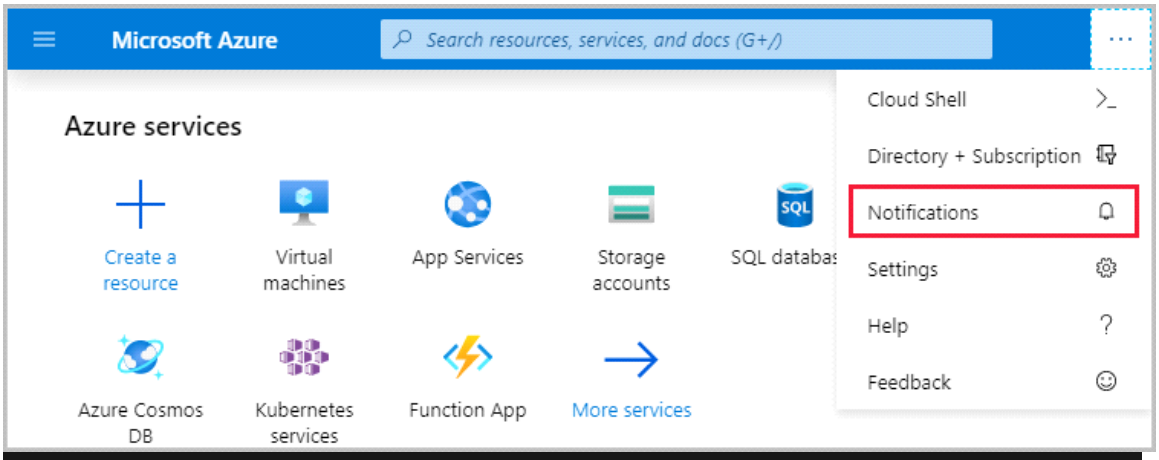
If you encounter an issue when you create the resources, verify you've selected the F1 pricing tier in the new App Service plan. Using the F1 pricing tier is a requirement of the sandbox system when you create this WordPress site.

Verify your website is running

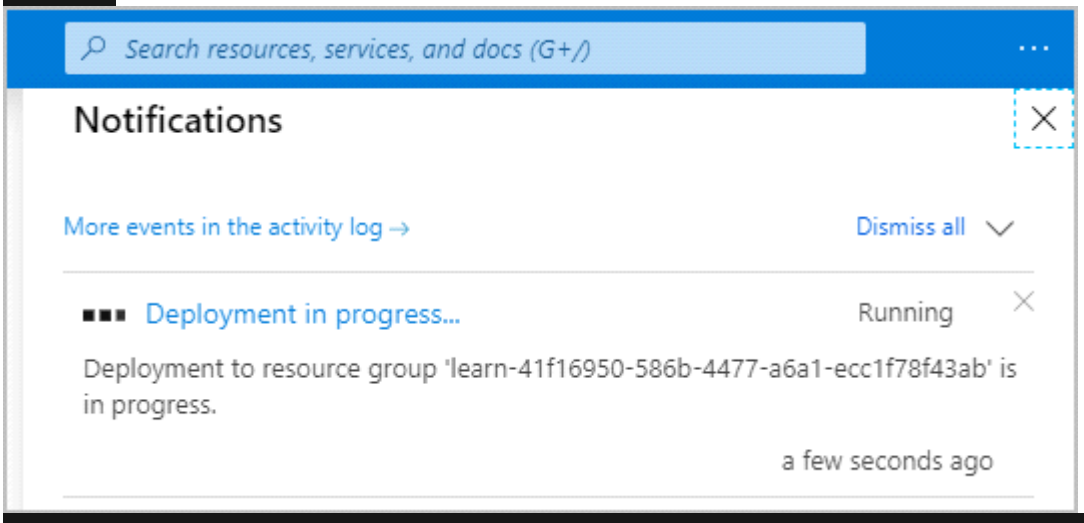
The deployment of the new website can take a few minutes to complete. You're welcome to explore the portal further on your own.

We can track the progress of the deployment at any time.

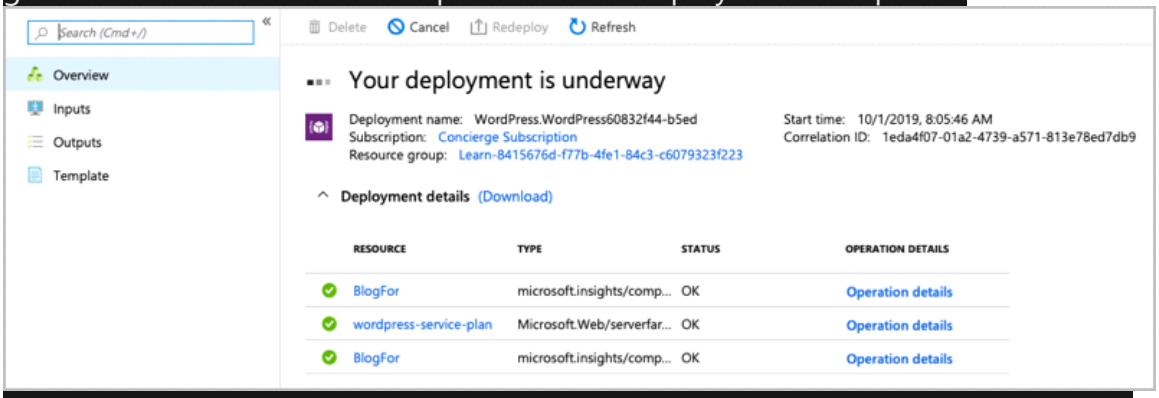
1. Select the Notifications bell icon at the top of the portal. If your browser window width is smaller, it might be shown when you select the ellipsis (...) icon in the upper-right corner.



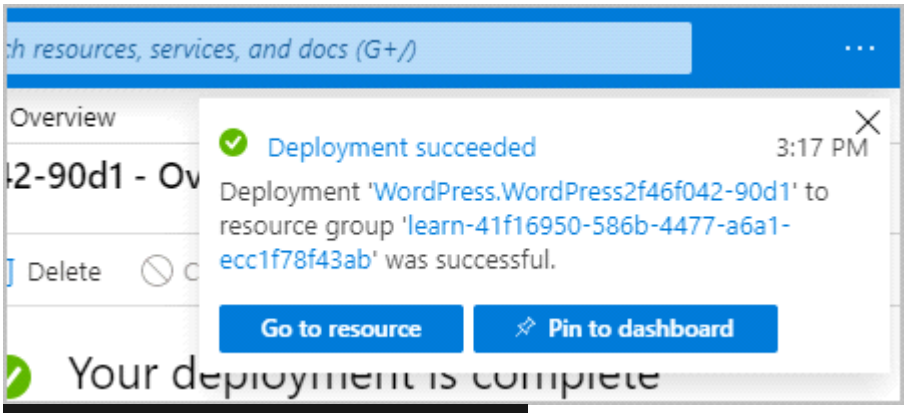
2. Select Deployment in progress to see the details about all the resources that are created.



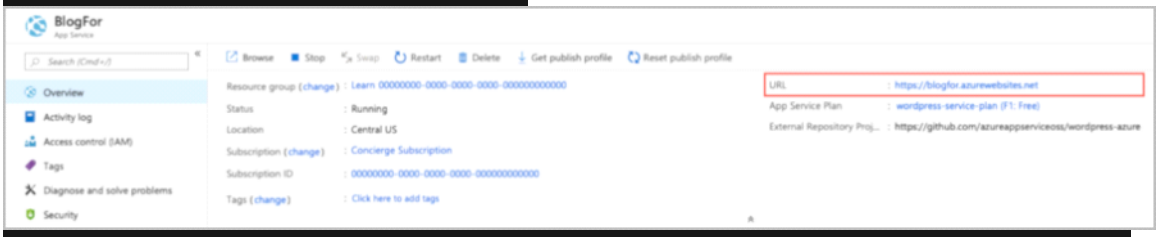
Notice how resources are listed as they're created and the status changes to a green check mark as each component in the deployment completes.



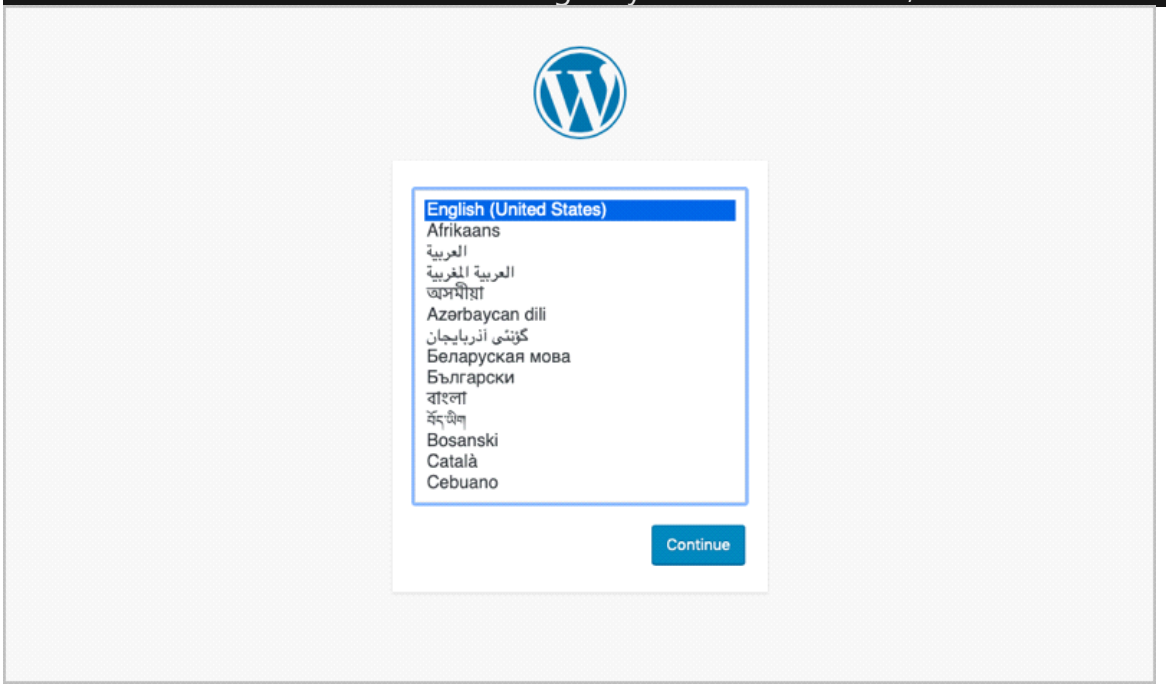
3. After the deployment status message changes to Your deployment is complete, you'll notice the status in the Notifications dialog box changes to Deployment succeeded. Select Go to resource to go to the App Service overview.



4. Find the URL in the Overview section.



5. Copy the URL information by selecting the Copy to clipboard icon at the end of URL.
6. Open a new tab in your browser, paste this URL, and press Enter to browse to your new WordPress site. You can now configure your WordPress site, and add content.



From <https://docs.microsoft.com/en-us/learn/modules/azure-architecture-fundamentals/exercise-create-website>

Part 2: Describe core Azure services

Thursday, January 28, 2021 10:19 AM

Explore Azure database and analytics services

Thursday, January 28, 2021 10:19 AM

In this module, you'll learn about several of the database services that are available on Microsoft Azure, such as Azure Cosmos DB, Azure SQL Database, Azure SQL Managed Instance, Azure Database for MySQL, and Azure Database for PostgreSQL. In addition, you'll learn about several of the big data and analysis services in Azure.

Overview

- Introduction 2 min
- Explore Azure Cosmos DB 4 min
- Explore Azure SQL Database 4 min
- Exercise - Create a SQL database 12 min
- Explore Azure SQL Managed Instance 4 min
- Explore Azure database for MySQL 4 min
- Explore Azure Database for PostgreSQL 4 min
- Explore big data and analytics 4 min
- Knowledge check 3 min
- Summary 2 min

From <https://docs.microsoft.com/en-us/learn/paths/az-900-describe-core-azure-services/>

Introduction

- 2 minutes

Due to a growing number of acquisitions over the last decade, Tailwind Traders uses a variety of database and analytics technologies. As the company begins to migrate existing data workloads and deploy new data workloads to Azure, it needs to understand which Azure technology will be appropriate for each workload. The company's Chief Technology Officer (CTO) has assigned you the task of researching the different database options that are available. This will help your company choose the right options for each of your data scenarios.

Today's applications are required to be highly responsive and always online. To achieve low latency and high availability, instances of these applications need to be deployed in datacenters that are close to their users. Applications need to respond in real time to large changes in usage at peak hours, store ever-increasing volumes of data, and make this data available to users in milliseconds. To help your company reach its goals, Azure database services are globally distributed, and Azure supports many of the industry

standard databases and APIs.
In this module, you'll learn about several of the primary database services that are available on Azure, and you'll analyze some of the reasons why each of these database services might be the right choice for your needs.

Learning objectives

After completing this module, you'll be able to describe the benefits and usage of:

- Azure Cosmos DB
- Azure SQL Database
- Azure SQL Managed Instance
- Azure Database for MySQL
- Azure Database for PostgreSQL
- Azure Synapse Analytics
- Azure HDInsight
- Azure Databricks
- Azure Data Lake Analytics

Prerequisites

- You should be familiar with basic computing concepts and terminology.
- You should be familiar with basic database concepts and terminology.

From <https://docs.microsoft.com/en-us/learn/modules/azure-database-fundamentals/introduction>

Explore Azure Cosmos DB

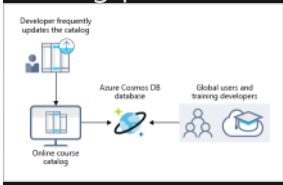
- 4 minutes

Over the years, Tailwind Traders has acquired several smaller companies. Each of these companies had teams of developers who used different database services and various APIs to work with their data. A long-term plan might be to eventually move all of the disparate data to a common database service. For now, though, you'd like to enable each of these teams to work with an environment where they can use their existing skills. Fortunately for you, Azure Cosmos DB can help out.

Azure Cosmos DB is a globally distributed, multi-model database service. You can elastically and independently scale throughput and storage across any number of Azure regions worldwide. You can take advantage of fast, single-digit-millisecond data access by using any one of several popular APIs. Azure Cosmos DB provides comprehensive service level agreements for throughput, latency, availability, and consistency guarantees.

Azure Cosmos DB supports schema-less data, which lets you build highly responsive and "Always On" applications to support constantly changing data. You can use this feature to store data that's updated and maintained by users around the world.

For example, Tailwind Traders provides a public training portal that is used by customers across the globe to learn about the different tools that Tailwind Traders creates. Tailwind Traders developers maintain and update the data. The following illustration shows a sample Azure Cosmos DB database that's used to store data for the Tailwind Traders training portal website.



Azure Cosmos DB is flexible. At the lowest level, Azure Cosmos DB stores data in atom-record-sequence (ARS) format. The data is then abstracted and projected as an API, which you specify when you're creating your database. Your choices include SQL, MongoDB, Cassandra, Tables, and Gremlin. This level of flexibility means that as you migrate your company's databases to Azure Cosmos DB, your developers can stick with the API that they're the most comfortable with.

From <https://docs.microsoft.com/en-us/learn/modules/azure-database-fundamentals/azure-cosmos-db>

Explore Azure SQL Database

- 4 minutes

Azure SQL Database is a relational database based on the latest stable version of the Microsoft SQL Server database engine. SQL Database is a high-performance, reliable, fully managed, and secure database. You can use it to build data-driven applications and websites in the programming language of your choice, without needing to manage infrastructure.

Features

Azure SQL Database is a platform as a service (PaaS) database engine. It handles most of the database management functions, such as upgrading, patching, backups, and monitoring, without user involvement. SQL Database provides 99.99 percent availability. PaaS capabilities that are built into SQL Database enable you to focus on the domain-specific database administration and optimization activities that are critical for your business. SQL Database is a fully managed service that has built-in high availability, backups, and other common maintenance operations. Microsoft handles all updates to the SQL and operating system code. You don't have to manage the underlying infrastructure.

You can create a highly available and high-performance data storage layer for the applications and solutions in Azure. SQL Database can be the right choice for a variety of modern cloud applications because it enables you to process both relational data and non-relational structures, such as graphs, JSON, spatial, and XML.

You can use advanced query processing features, such as high-performance, in-memory technologies and intelligent query processing. In fact, the newest capabilities of SQL Server are released first to SQL Database, and then to SQL Server itself. You get the newest SQL Server capabilities, with no overhead for updates or upgrades, tested across millions of databases.

Migration

Tailwind Traders currently uses several on-premises servers running SQL Server, which provide data storage for your public-facing website (for example, customer data, order history, and product catalogs). In addition, your on-premises servers running SQL Server also provide data storage for your internal-only training portal website. Tailwind Traders uses the website for new employee training materials (such as study materials, certification details, and training transcripts). The following illustration shows the types of data that your company might store in the Azure SQL Database training portal website.

You can migrate your existing SQL Server databases with minimal downtime by using the Azure Database Migration Service. The Microsoft Data Migration Assistant can generate assessment reports that provide recommendations to help guide you through required changes prior to performing a migration. After you assess and resolve any remediation required, you're ready to begin the migration process. The Azure Database Migration Service performs all of the required steps. You just change the connection string in your apps.

From <https://docs.microsoft.com/en-us/learn/modules/azure-database-fundamentals/azure-sql-database>

Exercise - Create a SQL database

- 12 minutes

This module requires a sandbox to complete. A sandbox gives you access to free resources. Your personal subscription will not be charged. The sandbox may only be used to complete training on Microsoft Learn. Use for any other reason is prohibited, and may result in permanent loss of access to the sandbox.

Sign in to activate sandbox

Tailwind Traders has chosen Azure SQL Database for part of its migration. You've been tasked with creating the database.

In this exercise, you'll create a SQL database in Azure and then query the data in that database.

Task 1: Create the database

In this task, you create a SQL database based on the *AdventureWorksLT* sample database.

1. Sign in to the Azure portal .
2. Select Create a resource > Databases > SQL database. Fill in the following information.

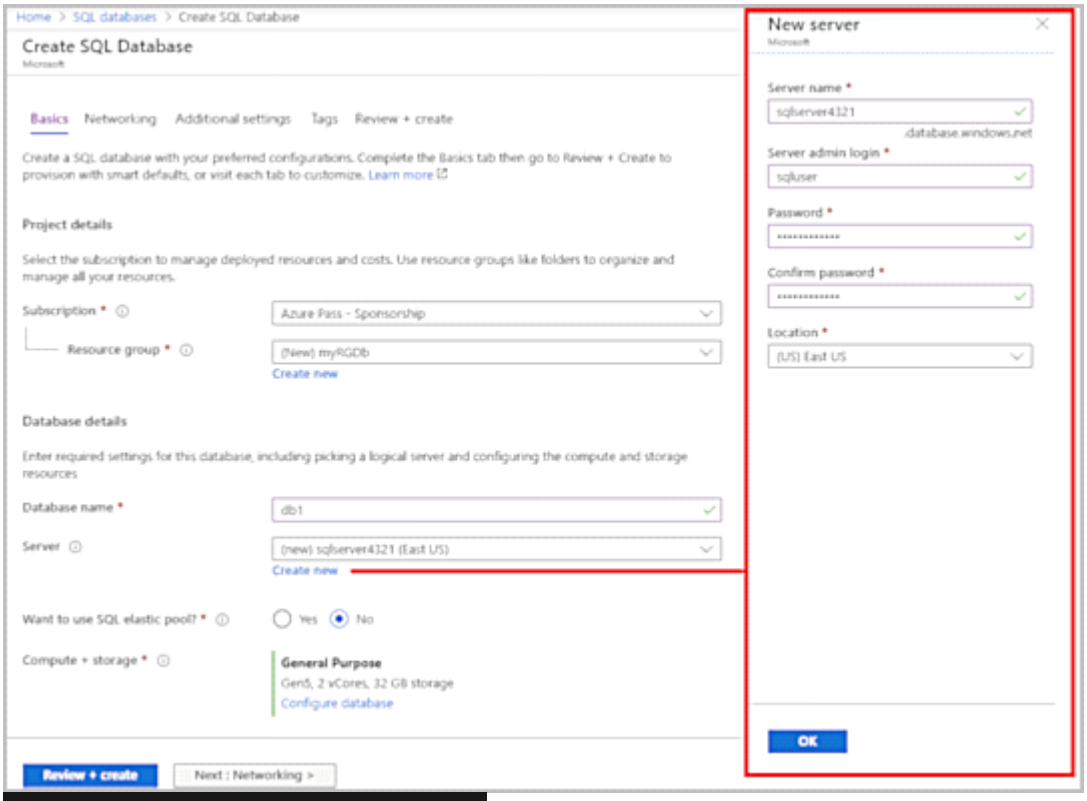
Setting	Value
On the Basics tab, under Project details section:	
Subscription	Concierge Subscription
Resource group	[sandbox resource group name]
Under Database details section:	
Database name	db1
Server	Select Create new.

TABLE 1

3. The New server panel appears. Enter the following information (replace nnnn in the name of the server with letters and digits, such that the name is globally unique).

Setting	Value
Server name	sqlservernnnn (must be unique)
Server admin login	sqluser
Password	Pa$$w0rd1234
Location	(US) East US

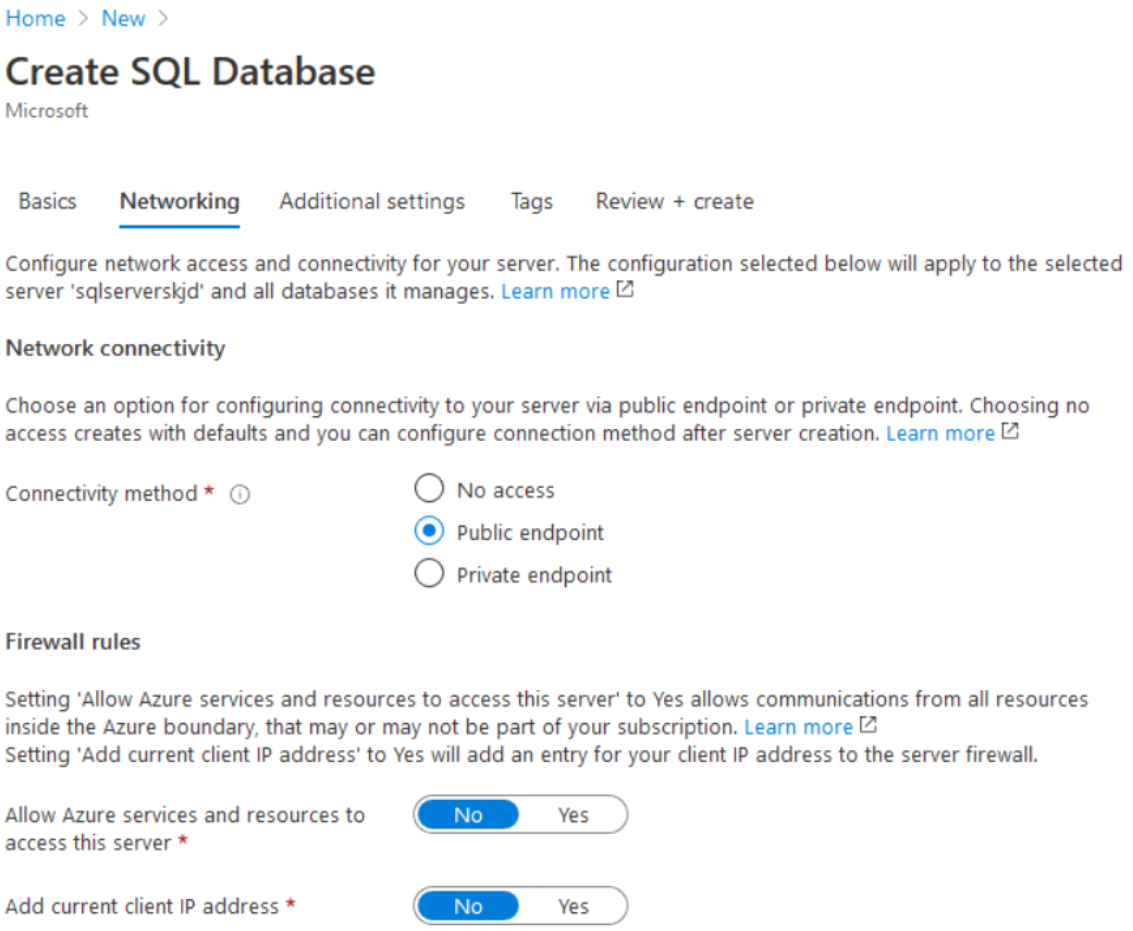
TABLE 2



4. Select OK when you have finished.
5. Select Next : Networking, and configure the following settings (leave defaults for remainder of fields).

Setting	**Value**
Under Network connectivity section:	
Connectivity method	Public endpoint (*default*)

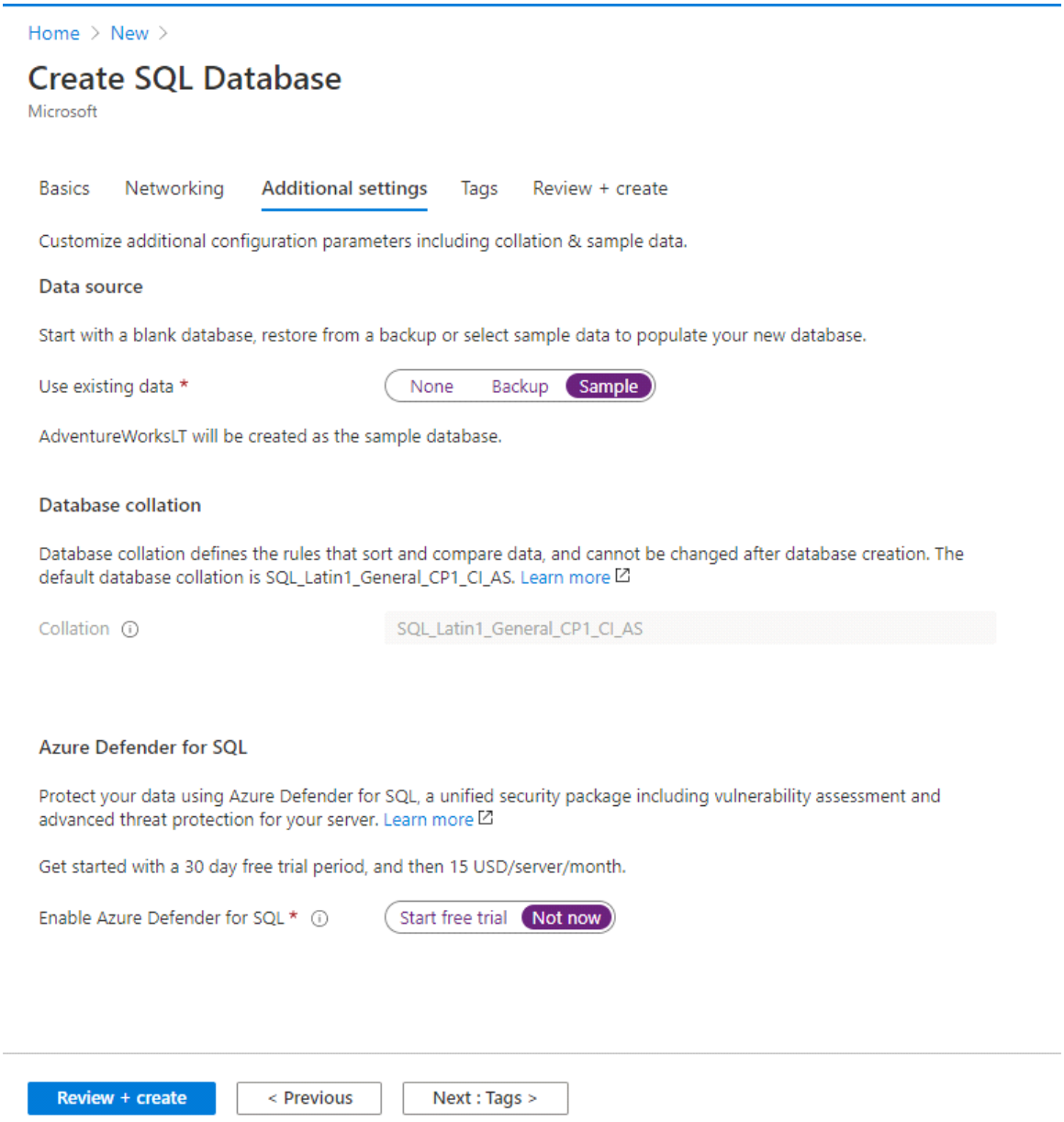
TABLE 3



6. Select Next : Additional settings, and configure the following settings.

Setting	Value
Under Data source section:	
Use existing data	Sample (this will create the *AdventureWorksLT* sample database)
Under Database collation section:	
Collation	*default*
Under Azure Defender for SQL section:	
Enable Azure Defender for SQL	Not now

TABLE 4



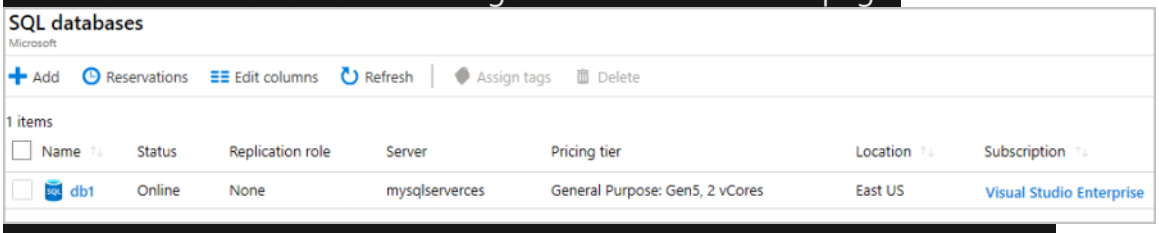
7. Select Review + create.
8. After validation success, on the Create SQL Database window, select Create to deploy the server and database.
   It can take approximately two to five minutes to create the server and deploy the sample database.
9. Select Go to resource.
10. Select Set server firewall, and then select Yes to Allow Azure services and resources to access this server.
11. Select Save.
12. Select OK.

Task 2: Test the database

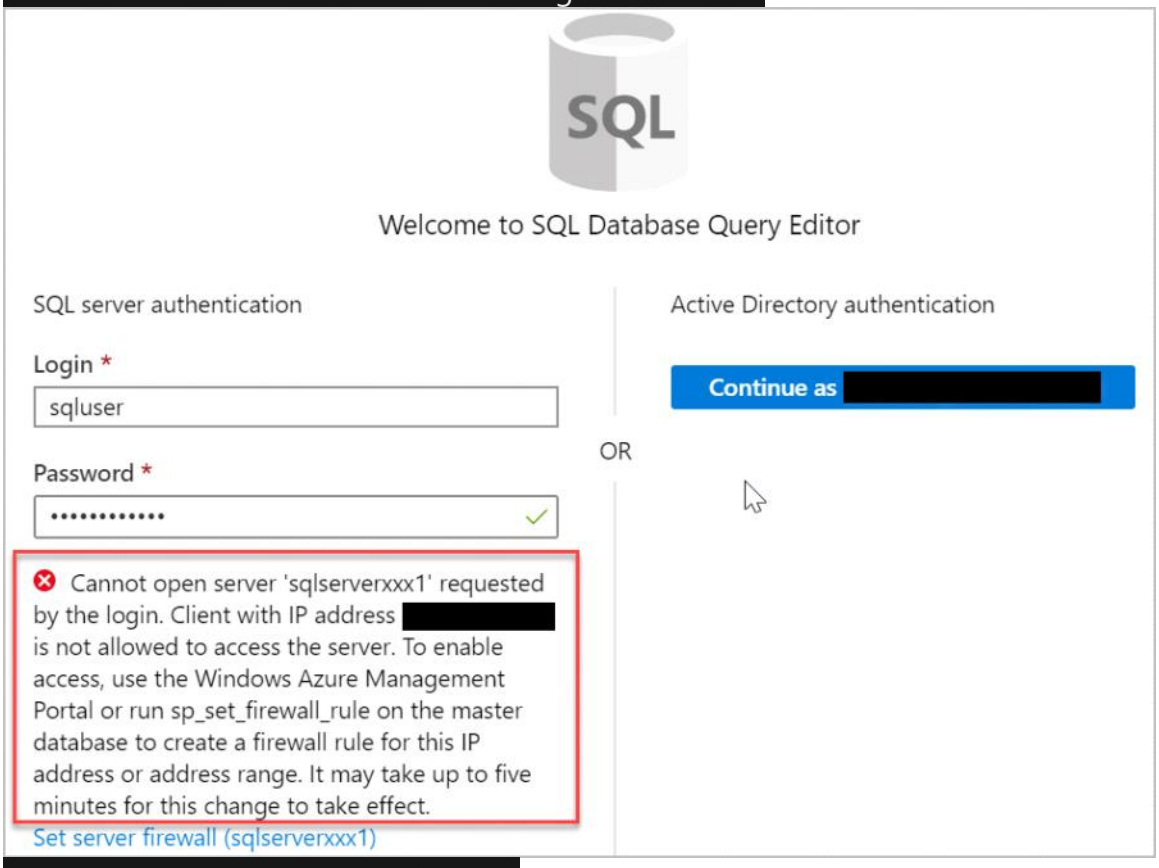
In this task, you configure the server and run a SQL query.

1. From the All resources pane, search and select SQL databases and ensure that your

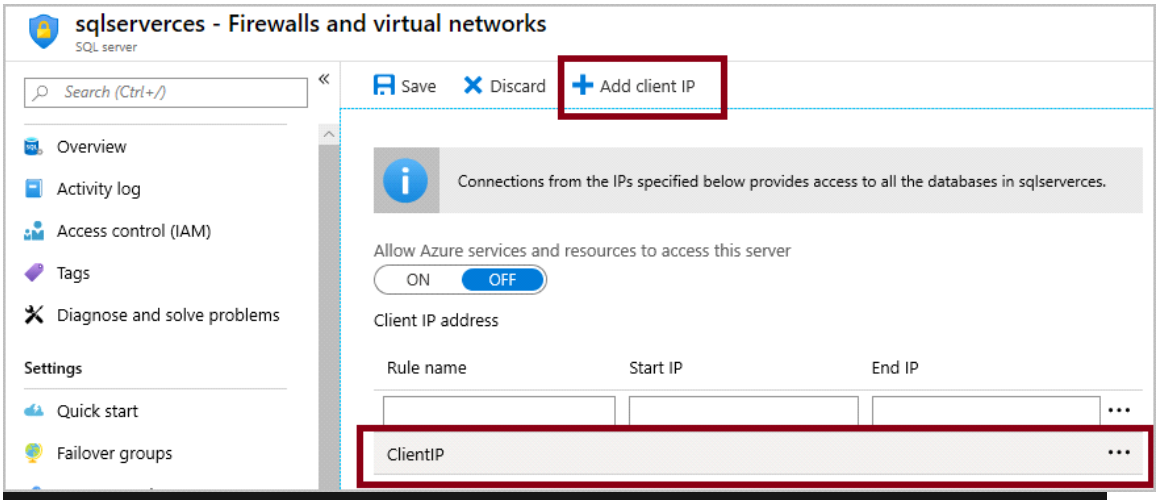
new database was created. You might need to refresh the page.



2. Select the db1 entry representing the SQL database you created, and then select Query editor (preview) in the nav bar.
3. Sign in as sqluser, with the password Pa$$w0rd1234.
4. You will not be able to sign in. Read the error closely and make note of the IP address that needs to be allowed through the firewall.



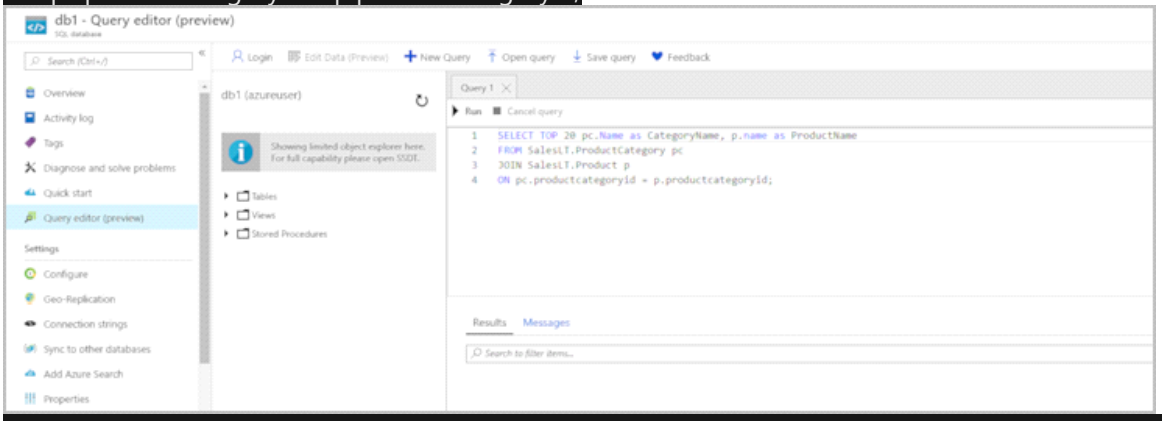
5. Select Overview > Set server firewall.
6. In Client IP address your IP will be shown. Select Rule name, add your IP in both the Start IP and End IP fields, and then select Save.



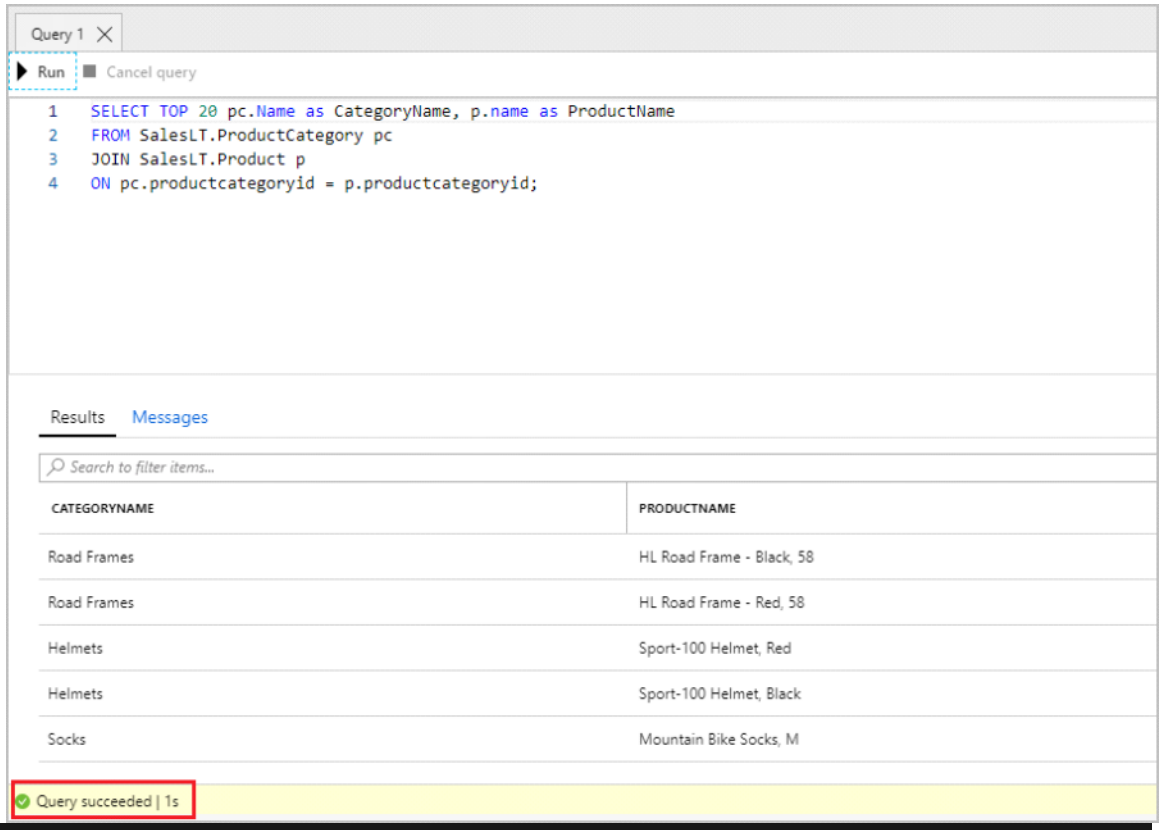
7. Return to your SQL database and the Query Editor sign-in page. Try to sign in again as sqluser, with the password Pa$$w0rd1234. This time you should succeed. It might take a couple of minutes for the new firewall rule to be deployed. If you wait and still get an error, try selecting Firewall settings > again.
8. After you sign in successfully, the query pane appears. Enter the following query into the editor pane.

SQLCopy

```
SELECT TOP 20 pc.Name as CategoryName, p.name as ProductName
FROM SalesLT.ProductCategory pc
JOIN SalesLT.Product p
ON pc.productcategoryid = p.productcategoryid;
```



9. Select Run, and then review the query results in the Results pane. The query should run successfully.



Congratulations! You've created a SQL database in Azure and successfully queried the data in that database.

From <https://docs.microsoft.com/en-us/learn/modules/azure-database-fundamentals/exercise-create-sql-database>

Explore Azure SQL Managed Instance

- 4 minutes

Azure SQL Managed Instance is a scalable cloud data service that provides the broadest SQL Server database engine compatibility with all the benefits of a fully managed platform as a service. Depending on your scenario, Azure SQL Managed Instance might offer more options for your database needs.

Features

Like Azure SQL Database, Azure SQL Managed Instance is a platform as a service (PaaS) database engine, which means that your company will be able to take advantage of the

best features of moving your data to the cloud in a fully-managed environment. For example, your company will no longer need to purchase and manage expensive hardware, and you won't have to maintain the additional overhead of managing your on-premises infrastructure. On the other hand, your company will benefit from the quick provisioning and service scaling features of Azure, together with automated patching and version upgrades. In addition, you'll be able to rest assured that your data will always be there when you need it through built-in high availability features and a 99.99% uptime service level agreement (SLA). You'll also be able to protect your data with automated backups and a configurable backup retention period.

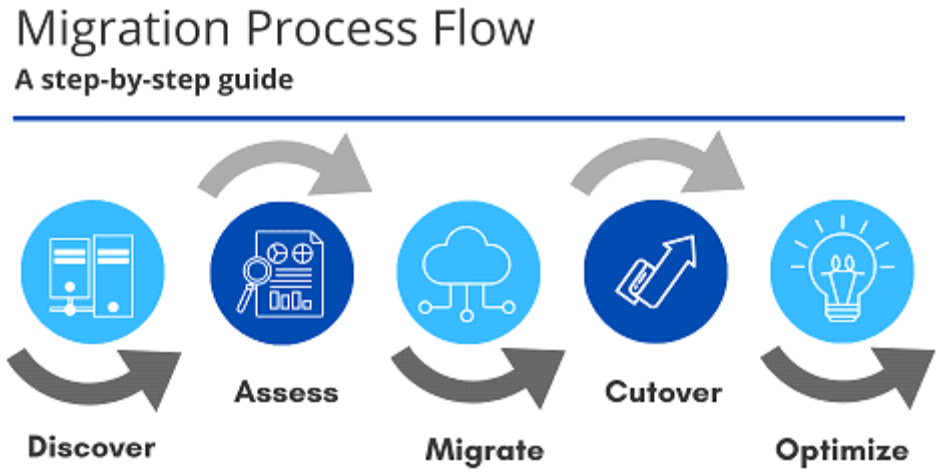
Azure SQL Database and Azure SQL Managed Instance offer many of the same features; however, Azure SQL Managed Instance provides several options that might not be available to Azure SQL Database. For example, Tailwind Traders currently uses several on-premises servers running SQL Server, and they would like to migrate their existing databases to a SQL database running in the cloud. However, several of their databases use Cyrillic characters for collation. In this scenario, Tailwind Traders should migrate their databases to an Azure SQL Managed Instance, since Azure SQL Database only uses the default SQL_Latin1_General_CP1_CI_AS server collation.

Note

For a detailed list of the differences between Azure SQL Database and Azure SQL Managed Instance, see Features comparison: Azure SQL Database and Azure SQL Managed Instance .

Migration

Azure SQL Managed Instance makes it easy to migrate your on-premises data on SQL Server to the cloud using the Azure Database Migration Service (DMS) or native backup and restore. After you have discovered all of the features that your company uses, you need to assess which on-premises SQL Server instances you can migrate to Azure SQL Managed Instance to see if you have any blocking issues. Once you have resolved any issues, you can migrate your data, then cutover from your on-premises SQL Server to your Azure SQL Managed Instance by changing the connection string in your applications.



Note

For a detailed description of the migration process, see Migration guide: SQL Server to SQL Managed Instance

From <https://docs.microsoft.com/en-us/learn/modules/azure-database-fundamentals/azure-sql-managed-instance>

Explore Azure database for MySQL

- 4 minutes

Tailwind Traders currently manages several websites on-premises that use the LAMP stack (Linux, Apache, MySQL, PHP). As part of your planning for your migration strategy, the different teams at Tailwind Traders have been researching the available service offerings that Azure provides. You've already discovered that the Web Apps feature of Azure App Service provides built-in functionality to create web applications that use PHP on a Linux server running Apache. You've been tasked with investigating whether the database requirements for the web development team will continue to be met after the migration to Azure.

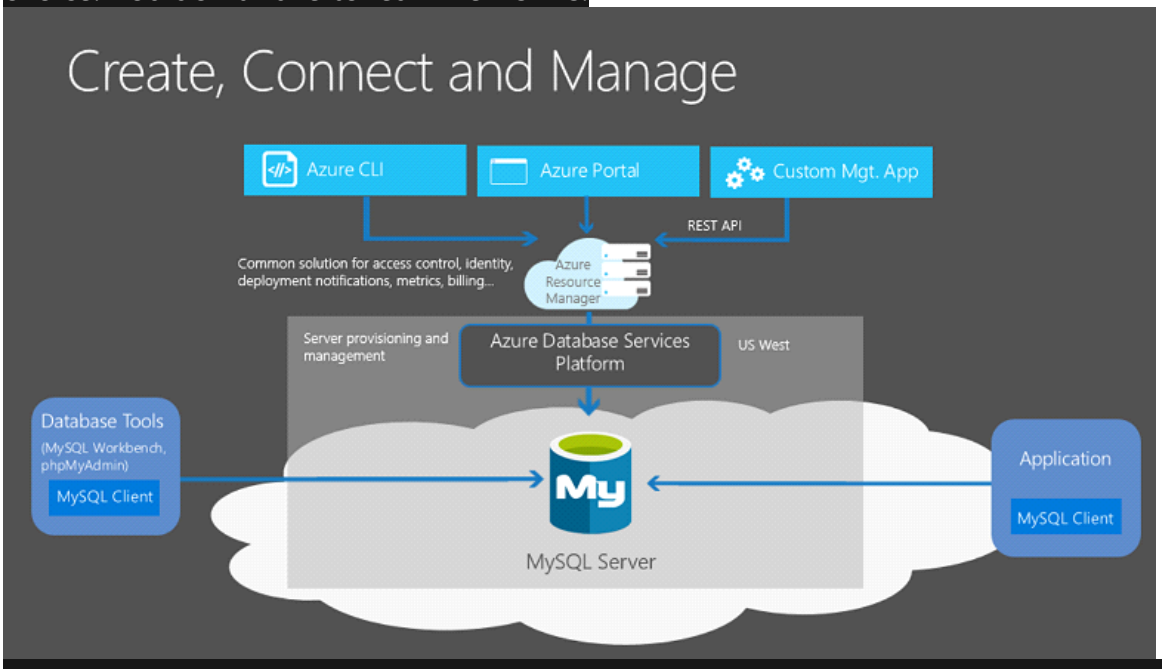
Azure Database for MySQL is a relational database service in the cloud, and it's based on the MySQL Community Edition database engine, versions 5.6, 5.7, and 8.0. With it, you have a 99.99 percent availability service level agreement from Azure, powered by a global network of Microsoft-managed datacenters. This helps keep your app running 24/7. With every Azure Database for MySQL server, you take advantage of built-in security, fault tolerance, and data protection that you would otherwise have to buy or design, build, and manage. With Azure Database for MySQL, you can use point-in-time restore to recover a server to an earlier state, as far back as 35 days.

Azure Database for MySQL delivers:

- Built-in high availability with no additional cost.
- Predictable performance and inclusive, pay-as-you-go pricing.
- Scale as needed, within seconds.
- Ability to protect sensitive data at-rest and in-motion.
- Automatic backups.
- Enterprise-grade security and compliance.

These capabilities require almost no administration, and all are provided at no additional cost. They allow you to focus on rapid app development and accelerating your time-to-market, rather than having to manage virtual machines and infrastructure. In addition, you can migrate your existing MySQL databases with minimal downtime by using the Azure Database Migration Service. After you have completed your migration, you can continue to develop your application with the open-source tools and platform of your

choice. You don't have to learn new skills.



Azure Database for MySQL offers several service tiers, and each tier provides different performance and capabilities to support lightweight to heavyweight database workloads. You can build your first app on a small database for a few dollars a month, and then adjust the scale to meet the needs of your solution. Dynamic scalability enables your database to transparently respond to rapidly changing resource requirements. You only pay for the resources you need, and only when you need them.

From <https://docs.microsoft.com/en-us/learn/modules/azure-database-fundamentals/azure-mysql-database>

Explore Azure Database for PostgreSQL

- 4 minutes

As part of its overall data strategy, Tailwind Traders have been using PostgreSQL for several years. You and your team probably already know the benefits of PostgreSQL. Part of your migration is to use Azure Database for PostgreSQL, and you want to make sure that you'll have access to the same benefits as your on-premises server before moving to the cloud.

Azure Database for PostgreSQL is a relational database service in the cloud. The server software is based on the community version of the open-source PostgreSQL database engine. Your familiarity with tools and expertise with PostgreSQL is applicable when

you're using Azure Database for PostgreSQL.

Moreover, Azure Database for PostgreSQL delivers the following benefits:

- Built-in high availability compared to on-premises resources. There's no additional configuration, replication, or cost required to make sure your applications are always available.
- Simple and flexible pricing. You have predictable performance based on a selected pricing tier choice that includes software patching, automatic backups, monitoring, and security.
- Scale up or down as needed, within seconds. You can scale compute or storage independently as needed, to make sure you adapt your service to match usage.
- Adjustable automatic backups and point-in-time-restore for up to 35 days.
- Enterprise-grade security and compliance to protect sensitive data at-rest and in-motion. This security covers data encryption on disk and SSL encryption between client and server communication.

Azure Database for PostgreSQL is available in two deployment options: Single Server and Hyperscale (Citus).

Single Server

The Single Server deployment option delivers:

- Built-in high availability with no additional cost (99.99 percent SLA).
- Predictable performance and inclusive, pay-as-you-go pricing.
- Vertical scale as needed, within seconds.
- Monitoring and alerting to assess your server.
- Enterprise-grade security and compliance.
- Ability to protect sensitive data at-rest and in-motion.
- Automatic backups and point-in-time-restore for up to 35 days.

All those capabilities require almost no administration, and all are provided at no additional cost. You can focus on rapid application development and accelerating your time to market, rather than having to manage virtual machines and infrastructure. You can continue to develop your application with the open-source tools and platform of your choice, without having to learn new skills.

The Single Server deployment option offers three pricing tiers: Basic, General Purpose, and Memory Optimized. Each tier offers different resource capabilities to support your database workloads. You can build your first app on a small database for a few dollars a month, and then adjust the scale to meet the needs of your solution. Dynamic scalability enables your database to transparently respond to rapidly changing resource requirements. You only pay for the resources you need, and only when you need them.

Hyperscale (Citus)

The Hyperscale (Citus) option horizontally scales queries across multiple machines by using sharding. Its query engine parallelizes incoming SQL queries across these servers for faster responses on large datasets. It serves applications that require greater scale and performance, generally workloads that are approaching, or already exceed, 100 GB of data.

The Hyperscale (Citus) deployment option supports multi-tenant applications, real-time operational analytics, and high throughput transactional workloads. Applications built for PostgreSQL can run distributed queries on Hyperscale (Citus) with standard

connection libraries and minimal changes.

From <https://docs.microsoft.com/en-us/learn/modules/azure-database-fundamentals/azure-postgresql-database>

Explore big data and analytics

- 4 minutes

Several years ago, Tailwind Traders rolled out a new GPS tracking system for all of its delivery vehicles. The new system provides real-time tracking data to your primary datacenter. Your CTO wants your team to look at several years of tracking data in order to determine trends. For example, an important trend might be a spike in deliveries around the holidays that would require hiring additional staff. Through an in-depth analysis of the tracking data that you've recorded, your CTO seeks to predict when changes are necessary, and proactively take the steps that are necessary to manage spikes appropriately.

Data comes in all types of forms and formats. When we talk about big data, we're referring to large volumes of data. In this Tailwind Traders scenario, data is collected from the GPS sensors, which includes location information, data from weather systems, and many other sources that generate large amounts of data. This amount of data becomes increasingly hard to make sense of and to base decisions on. The volumes are so large that traditional forms of processing and analysis are no longer appropriate.

Open-source cluster technologies have been developed, over time, to try to deal with these large datasets. Microsoft Azure supports a broad range of technologies and services to provide big data and analytic solutions, including Azure Synapse Analytics, Azure HDInsight, Azure Databricks, and Azure Data Lake Analytics.

Azure Synapse Analytics

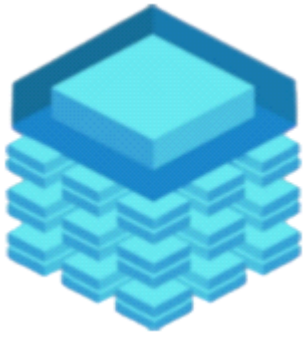
Azure Synapse Analytics (formerly Azure SQL Data Warehouse) is a limitless analytics service that brings together enterprise data warehousing and big data analytics. You can query data on your terms by using either serverless or provisioned resources at scale. You have a unified experience to ingest, prepare, manage, and serve data for immediate BI and machine learning needs.

Azure HDInsight

Azure HDInsight is a fully managed, open-source analytics service for enterprises. It's a cloud service that makes it easier, faster, and more cost-effective to process massive amounts of data. You can run popular open-source frameworks and create cluster types such as Apache Spark, Apache Hadoop, Apache Kafka, Apache HBase, Apache Storm, and Machine Learning Services. HDInsight also supports a broad range of scenarios such as extraction, transformation, and loading (ETL), data warehousing, machine learning, and IoT.

Azure Databricks

Azure Databricks helps you unlock insights from all your data and build artificial intelligence solutions. You can set up your Apache Spark environment in minutes, and then autoscale and collaborate on shared projects in an interactive workspace. Azure Databricks supports Python, Scala, R, Java, and SQL, as well as data science frameworks and libraries including TensorFlow, PyTorch, and scikit-learn.



Azure Data Lake Analytics

Azure Data Lake Analytics is an on-demand analytics job service that simplifies big data. Instead of deploying, configuring, and tuning hardware, you write queries to transform your data and extract valuable insights. The analytics service can handle jobs of any scale instantly by setting the dial for how much power you need. You only pay for your job when it's running, making it more cost-effective.

From <https://docs.microsoft.com/en-us/learn/modules/azure-database-fundamentals/azure-big-data-analytics>

Explore Azure compute services

Thursday, January 28, 2021 10:22 AM

In this module, you'll learn how to take advantage of several virtualization services in Azure compute, which can help your applications scale out quickly and efficiently to meet increasing demands.

Overview

- Introduction 2 min
- Overview of Azure compute services 4 min
- When to use Azure Virtual Machines 8 min
- When to use Azure Container Instances or Azure Kubernetes Service 12 min
- When to use Azure App Service 3 min
- When to use Azure Functions 10 min
- When to use Windows Virtual Desktop 9 min
- Knowledge check 3 min
- Summary 1 min

From <https://docs.microsoft.com/en-us/learn/paths/az-900-describe-core-azure-services/>

Introduction

- 2 minutes

Imagine that you work as a development lead at Tailwind Traders, a company that specializes in hardware manufacturing. Your management team tells you that the company's website has been having a difficult time keeping up with the application demands. The team wants you to investigate a solution. The front-end web servers are operating near capacity during peak periods of the day, and you need to get a solution in place quickly. But there's a problem. You don't have any free servers to scale out your application.

You could ask to buy new equipment, but your department's budget is tight. You want to make a good impression with leadership, but you don't know how many servers are necessary for this project, and you don't want to buy more hardware than you need. Even if you were able to procure several servers, you'd need to invest a lot of time to set them up and install software.

Ideally, you'd obtain the resources you need to do the work without too much administration and configure them to do the work. You'd also pay only for the compute resources you need while you're using them.

This scenario is exactly what you can do in Azure. You can create compute resources, configure them to do the work that's needed, and pay for only what you use.

Learning objectives

After completing this module, you'll be able to describe the benefits and usage of:

- Azure Virtual Machines
- Azure App Service

- Azure Container Instances
- Azure Kubernetes Service
- Azure Functions
- Windows Virtual Desktop

Prerequisites

- You should be familiar with basic computing concepts and terminology.
- Familiarity with cloud computing is helpful but isn't necessary.

From <https://docs.microsoft.com/en-us/learn/modules/azure-compute-fundamentals/introduction>

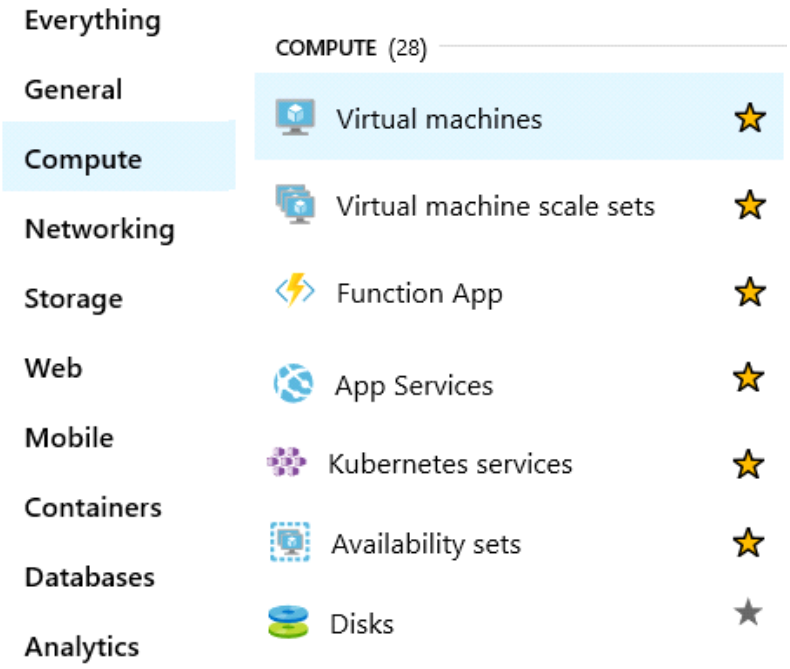
Overview of Azure compute services

- 4 minutes

Azure compute is an on-demand computing service for running cloud-based applications. It provides computing resources such as disks, processors, memory, networking, and operating systems. The resources are available on-demand and can typically be made available in minutes or even seconds. You pay only for the resources you use, and only for as long as you're using them.

Azure supports a wide range of computing solutions for development and testing, running applications, and extending your datacenter. The service supports Linux, Windows Server, SQL Server, Oracle, IBM, and SAP. Azure also has many services that can run virtual machines (VMs). Each service provides different options depending on your requirements. Some of the most prominent services are:

- Azure Virtual Machines
- Azure Container Instances
- Azure App Service
- Azure Functions (or *serverless computing*)



Virtual machines

Virtual machines are software emulations of physical computers. They include a virtual processor, memory, storage, and networking

resources. VMs host an operating system, and you can install and run software just like a physical computer. When using a remote desktop client, you can use and control the VM as if you were sitting in front of it.
With Azure Virtual Machines , you can create and use VMs in the cloud. Virtual Machines provides infrastructure as a service (IaaS) and can be used in different ways. When you need total control over an operating system and environment, VMs are an ideal choice. Just like a physical computer, you can customize all the software running on the VM. This ability is helpful when you're running custom software or custom hosting configurations.

Virtual machine scale sets

Virtual machine scale sets are an Azure compute resource that you can use to deploy and manage a set of identical VMs. With all VMs configured the same, virtual machine scale sets are designed to support true autoscale. No pre-provisioning of VMs is required. For this reason, it's easier to build large-scale services targeting big compute, big data, and containerized workloads. As demand goes up, more VM instances can be added. As demand goes down, VM instances can be removed. The process can be manual, automated, or a combination of both.

Containers and Kubernetes

Container Instances and Azure Kubernetes Service are Azure compute resources that you can use to deploy and manage containers. Containers are lightweight, virtualized application environments. They're designed to be quickly created, scaled out, and stopped dynamically. You can run multiple instances of a containerized application on a single host machine.

App Service

With Azure App Service , you can quickly build, deploy, and scale enterprise-grade web, mobile, and API apps running on any platform. You can meet rigorous performance, scalability, security, and compliance requirements while using a fully managed platform to perform infrastructure maintenance. App Service is a platform as a service (PaaS) offering.

Functions

Functions are ideal when you're concerned only about the code running your service and not the underlying platform or infrastructure. They're commonly used when you need to perform work in response to an event (often via a REST request), timer, or message from another Azure service, and when that work can be completed quickly, within seconds or less.

From <https://docs.microsoft.com/en-us/learn/modules/azure-compute-fundamentals/overview>

When to use Azure Virtual Machines

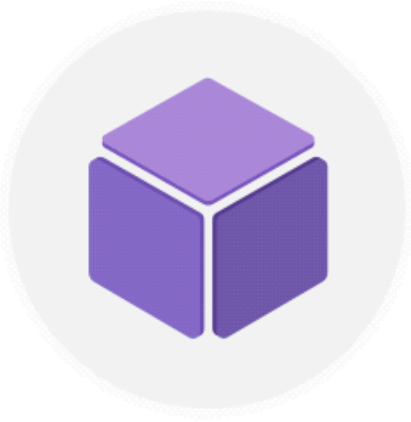
- 8 minutes

One possible solution to Tailwind Traders' lack of physical servers is through the use of virtual machines (VMs).

With Azure Virtual Machines, you can create and use VMs in the cloud. VMs provide infrastructure as a service (IaaS) in the form of a virtualized server and can be used in many ways. Just like a physical computer, you can customize all of the software running on the VM. VMs are an ideal choice when you need:

- Total control over the operating system (OS).
- The ability to run custom software.
- To use custom hosting configurations.

An Azure VM gives you the flexibility of virtualization without having to buy and maintain the physical hardware that runs the VM. You still need to configure, update, and maintain the software that runs on the VM.



You can create and provision a VM in minutes when you select a preconfigured VM image. Selecting an image is one of the most important decisions you'll make when you create a VM. An image is a template used to create a VM. These templates already include an OS and often other software, like development tools or web hosting environments.

Examples of when to use VMs

- During testing and development. VMs provide a quick and easy way to create different OS and application configurations. Test and development personnel can then easily delete the VMs when they no longer need them.
- When running applications in the cloud. The ability to run certain applications in the public cloud as opposed to creating a traditional infrastructure to run them can provide substantial economic benefits. For example, an application might need to handle fluctuations in demand. Shutting down VMs when you don't need them or quickly starting them up to meet a sudden increase in demand means you pay only for the resources you use.
- When extending your datacenter to the cloud. An organization can extend the capabilities of its own on-premises network by creating a virtual network in Azure and adding VMs to that virtual network. Applications like SharePoint can then run on an Azure VM instead of running locally. This arrangement makes it easier or less expensive to deploy than in an on-premises environment.

- During disaster recovery. As with running certain types of applications in the cloud and extending an on-premises network to the cloud, you can get significant cost savings by using an IaaS-based approach to disaster recovery. If a primary datacenter fails, you can create VMs running on Azure to run your critical applications and then shut them down when the primary datacenter becomes operational again.

Move to the cloud with VMs

VMs are also an excellent choice when you move from a physical server to the cloud (also known as lift and shift). You can create an image of the physical server and host it within a VM with little or no changes. Just like a physical on-premises server, you must maintain the VM. You update the installed OS and the software it runs.

Scale VMs in Azure

You can run single VMs for testing, development, or minor tasks. Or you can group VMs together to provide high availability, scalability, and redundancy. No matter what your uptime requirements are, Azure has several features that can meet them. These features include:

- Virtual machine scale sets
- Azure Batch

What are virtual machine scale sets?

Virtual machine scale sets let you create and manage a group of identical, load-balanced VMs. Imagine you're running a website that enables scientists to upload astronomy images that need to be processed. If you duplicated the VM, you'd normally need to configure an additional service to route requests between multiple instances of the website. Virtual machine scale sets could do that work for you.
Scale sets allow you to centrally manage, configure, and update a large number of VMs in minutes to provide highly available applications. The number of VM instances can automatically increase or decrease in response to demand or a defined schedule. With virtual machine scale sets, you can build large-scale services for areas such as compute, big data, and container workloads.

What is Azure Batch?

Azure Batch enables large-scale parallel and high-performance computing (HPC) batch jobs with the ability to scale to tens, hundreds, or thousands of VMs.
When you're ready to run a job, Batch does the following:

- Starts a pool of compute VMs for you.
- Installs applications and staging data.
- Runs jobs with as many tasks as you have.
- Identifies failures.
- Requeues work.
- Scales down the pool as work completes.

There might be situations in which you need raw computing power or supercomputer-level compute power. Azure provides these capabilities.

From <https://docs.microsoft.com/en-us/learn/modules/azure-compute-fundamentals/azure-virtual-machines>

When to use Azure Container Instances or Azure Kubernetes Service

- 12 minutes

While virtual machines are an excellent way to reduce costs versus the investments that are necessary for physical hardware, they're still limited to a single operating system per virtual machine. If you want to run multiple instances of an application on a single host machine, containers are an excellent choice.

What are containers?

Containers are a virtualization environment. Much like running multiple virtual machines on a single physical host, you can run multiple containers on a single physical or virtual host. Unlike virtual machines, you don't manage the operating system for a container. Virtual machines appear to be an instance of an operating system that you can connect to and manage, but containers are lightweight and designed to be created, scaled out, and stopped dynamically. While it's possible to create and deploy virtual machines as application demand increases, containers are designed to allow you to respond to changes on demand. With containers, you can quickly restart in case of a crash or hardware interruption. One of the most popular container engines is Docker, which is supported by Azure.

Compare virtual machines to containers

The following video highlights several of the important differences between virtual machines and containers.

Manage containers

Containers are managed through a container orchestrator, which can start, stop, and scale out application instances as needed. There are two ways to manage both Docker and Microsoft-based containers in Azure: Azure Container Instances and Azure Kubernetes Service (AKS).

Azure Container Instances

Azure Container Instances offers the fastest and simplest way to run a container in Azure without having to manage any virtual machines or adopt any additional services. It's a platform as a service (PaaS) offering that allows you to upload your containers, which it runs for you.

Azure Kubernetes Service

The task of automating, managing, and interacting with a large number of containers is known as orchestration. Azure Kubernetes Service is a complete orchestration service for containers with distributed architectures and large volumes of containers. Orchestration is the task of automating and managing a large number of containers and how they interact.

What is Kubernetes?

The following video discusses some important details about Kubernetes container orchestration.

Use containers in your solutions

Containers are often used to create solutions by using a *microservice architecture*. This architecture is where you break solutions into smaller, independent pieces. For example, you might split a website into a container hosting your front end, another hosting your back end, and a third for storage. This split allows you to separate portions of your app into logical sections that can be maintained, scaled, or updated independently. Imagine your website back-end has reached capacity but the front end and storage aren't being stressed. You could:

- Scale the back end separately to improve performance.
- Decide to use a different storage service.
- Replace the storage container without affecting the rest of the application.

What is a microservice?

The following video discusses some important details about microservices.

From <https://docs.microsoft.com/en-us/learn/modules/azure-compute-fundamentals/azure-container-services>

When to use Azure App Service

- 3 minutes

In your research for Tailwind Traders, you've looked at two different ways that you can virtualize your application. Another alternative is to deploy your application's front-end websites to Azure App Service, which makes it easy to respond to application demand.

App Service enables you to build and host web apps, background jobs, mobile back-ends, and RESTful APIs in the programming language of your choice without managing infrastructure. It offers automatic scaling and high availability. App Service supports Windows and Linux and enables automated deployments from GitHub, Azure DevOps, or any Git repo to support a continuous deployment model.

This platform as a service (PaaS) environment allows you to focus on the website and API logic while Azure handles the infrastructure to run and scale your web applications.

Azure App Service costs

You pay for the Azure compute resources your app uses while it processes requests based on the App Service plan you choose. The App Service plan determines how much hardware is devoted to your host. For example, the plan determines whether it's dedicated or shared hardware and how much memory is reserved for it. There's even a *free* tier you can use to host small, low-traffic sites.

Types of app services

With App Service, you can host most common app service styles like:

- Web apps
- API apps
- WebJobs
- Mobile apps

App Service handles most of the infrastructure decisions you deal with in hosting web-accessible apps:

- Deployment and management are integrated into the platform.
- Endpoints can be secured.
- Sites can be scaled quickly to handle high traffic loads.
- The built-in load balancing and traffic manager provide high availability.

All of these app styles are hosted in the same infrastructure and share these benefits. This flexibility makes App Service the ideal choice to host web-oriented applications.

Web apps

App Service includes full support for hosting web apps by using ASP.NET, ASP.NET Core, Java, Ruby, Node.js, PHP, or Python. You can choose either Windows or Linux as the host operating system.

API apps

Much like hosting a website, you can build REST-based web APIs by using your choice

of language and framework. You get full Swagger support and the ability to package and publish your API in Azure Marketplace. The produced apps can be consumed from any HTTP- or HTTPS-based client.

WebJobs

You can use the WebJobs feature to run a program (.exe, Java, PHP, Python, or Node.js) or script (.cmd, .bat, PowerShell, or Bash) in the same context as a web app, API app, or mobile app. They can be scheduled or run by a trigger. WebJobs are often used to run background tasks as part of your application logic.

Mobile apps

Use the Mobile Apps feature of App Service to quickly build a back end for iOS and Android apps. With just a few clicks in the Azure portal, you can:

- Store mobile app data in a cloud-based SQL database.
- Authenticate customers against common social providers, such as MSA, Google, Twitter, and Facebook.
- Send push notifications.
- Execute custom back-end logic in C# or Node.js.

On the mobile app side, there's SDK support for native iOS and Android, Xamarin, and React native apps.

From <https://docs.microsoft.com/en-us/learn/modules/azure-compute-fundamentals/azure-app-services>

When to use Azure Functions

- 10 minutes

After consulting with several of your fellow developers at Tailwind Traders, you've determined that some of your application logic is event driven. In other words, for a large amount of time, your application is waiting for a particular input before it performs any processing. To reduce your costs, you want to avoid having to pay for the time that your application is waiting for input. With that in mind, you've decided to investigate Azure Functions to see if it can help.

Serverless computing is the abstraction of servers, infrastructure, and operating systems. With serverless computing, Azure takes care of managing the server infrastructure and the allocation and deallocation of resources based on demand. Infrastructure isn't your responsibility. Scaling and performance are handled automatically. You're billed only for the exact resources you use. There's no need to even reserve capacity.

Serverless computing includes the abstraction of servers, an event-driven scale, and micro-billing:

- Abstraction of servers: Serverless computing abstracts the servers you run on. You never explicitly reserve server instances. The platform manages that for you. Each function execution can run on a different compute instance. This execution context is transparent to the code. With serverless architecture, you deploy your code, which then runs with high availability.
- Event-driven scale: Serverless computing is an excellent fit for workloads that respond to incoming events. Events include triggers by:
- Timers, for example, if a function needs to run every day at 10:00 AM UTC.
- HTTP, for example, API and webhook scenarios.
- Queues, for example, with order processing.
- And much more.
  Instead of writing an entire application, the developer authors a function, which contains both code and metadata about its triggers and bindings. The platform automatically schedules the function to run and scales the number of compute instances based on the rate of incoming events. Triggers define how a function is invoked. Bindings provide a declarative way to connect to services from within the code.
- Micro-billing: Traditional computing bills for a block of time like paying a monthly or annual rate for website hosting. This method of billing is convenient but isn't always cost effective. Even if a customer's website gets only one hit a day, they still pay for a full day's worth of availability. With serverless computing, they pay only for the time their code runs. If no active function executions occur, they're not charged. For example, if the code runs once a day for two minutes, they're charged for one execution and two minutes of computing time.

Serverless computing in Azure

Azure has two implementations of serverless compute:

- Azure Functions: Functions can execute code in almost any modern language.
- Azure Logic Apps: Logic apps are designed in a web-based designer and can execute logic triggered by Azure services without writing any code.

Azure Functions

When you're concerned only about the code running your service, and not the underlying platform or infrastructure, using Azure Functions is ideal. Functions are

commonly used when you need to perform work in response to an event (often via a REST request), timer, or message from another Azure service, and when that work can be completed quickly, within seconds or less.

Functions scale automatically based on demand, so they're a solid choice when demand is variable. For example, you might receive messages from an IoT solution that's used to monitor a fleet of delivery vehicles. You'll likely have more data arriving during business hours.

Using a virtual machine-based approach, you'd incur costs even when the virtual machine is idle. With functions, Azure runs your code when it's triggered and automatically deallocates resources when the function is finished. In this model, you're only charged for the CPU time used while your function runs.

Functions can be either stateless or stateful. When they're stateless (the default), they behave as if they're restarted every time they respond to an event. When they're stateful (called Durable Functions), a context is passed through the function to track prior activity.

Functions are a key component of serverless computing. They're also a general compute platform for running any type of code. If the needs of the developer's app change, you can deploy the project in an environment that isn't serverless. This flexibility allows you to manage scaling, run on virtual networks, and even completely isolate the functions.

Azure Logic Apps

Logic apps are similar to functions. Both enable you to trigger logic based on an event. Where functions execute code, logic apps execute *workflows* that are designed to automate business scenarios and are built from predefined logic blocks.

Every Azure logic app workflow starts with a trigger, which fires when a specific event happens or when newly available data meets specific criteria. Many triggers include basic scheduling capabilities, so developers can specify how regularly their workloads will run. Each time the trigger fires, the Logic Apps engine creates a logic app instance that runs the actions in the workflow. These actions can also include data conversions and flow controls, such as conditional statements, switch statements, loops, and branching.

You create logic app workflows by using a visual designer on the Azure portal or in Visual Studio. The workflows are persisted as a JSON file with a known workflow schema. Azure provides more than 200 different connectors and processing blocks to interact with different services. These resources include the most popular enterprise apps. You can also build custom connectors and workflow steps if the service you need to interact with isn't covered. You then use the visual designer to link connectors and blocks together. You pass data through the workflow to do custom processing, often all without writing any code.

As an example, let's say a ticket arrives in Zendesk. You could:

- Detect the intent of the message with cognitive services.
- Create an item in SharePoint to track the issue.
- Add the customer to your Dynamics 365 CRM system if they aren't already in your database.
- Send a follow-up email to acknowledge their request.

All of those actions could be designed in a visual designer, which makes it easy to see the logic flow. For this reason, it's ideal for a business analyst role.

Functions vs. Logic Apps

Functions and Logic Apps can both create complex orchestrations. An orchestration is a collection of functions or steps that are executed to accomplish a complex task.

- With Functions, you write code to complete each step.
- With Logic Apps, you use a GUI to define the actions and how they relate to one another.

You can mix and match services when you build an orchestration, calling functions from logic apps and calling logic apps from functions. Here are some common differences between the two.

	Functions	**Logic Apps**
State	Normally stateless, but Durable Functions provide state.	Stateful.
Development	Code-first (imperative).	Designer-first (declarative).
Connectivity	About a dozen built-in binding types. Write code for custom bindings.	Large collection of connectors. Enterprise Integration Pack for B2B scenarios. Build custom connectors.
Actions	Each activity is an Azure function. Write code for activity functions.	Large collection of ready-made actions.
Monitoring	Azure Application Insights.	Azure portal, Log Analytics.
Management	REST API, Visual Studio.	Azure portal, REST API, PowerShell, Visual Studio.
Execution context	Can run locally or in the cloud.	Runs only in the cloud.

FUNCTIONS VS. LOGIC APPS

From <https://docs.microsoft.com/en-us/learn/modules/azure-compute-fundamentals/azure-functions>

When to use Windows Virtual Desktop

- 9 minutes

In addition to the challenges that Tailwind Traders has been facing with application scale, your manager has asked you to put together a new development team of remote workers.

This task would normally require setting up several new computers with all of the requisite development tools for your new team. Then you would need to ship them to the respective developers across the country. The time to procure, set up, and ship each of these computers would be costly. Also, all of your new developers have their own computing devices that are running a mixture of Windows, Android, and macOS operating systems.

You want to find a way to expedite the deployment process for your remote workers. You also want to keep your management costs to a minimum. With that in mind, you want to see how Windows Virtual Desktop can help your organization.

What is Windows Virtual Desktop?

Windows Virtual Desktop on Azure is a desktop and application virtualization service that runs on the cloud. It enables your users to use a cloud-hosted version of Windows from any location. Windows Virtual Desktop works across devices like Windows, Mac, iOS, Android, and Linux. It works with apps that you can use to access remote desktops and apps. You can also use most modern browsers to access Windows Virtual Desktop-

hosted experiences.
The following video gives you an overview of Windows Virtual Desktop.

Why should you use Windows Virtual Desktop?

Provide the best user experience

Users have the freedom to connect to Windows Virtual Desktop with any device over the internet. They use a Windows Virtual Desktop client to connect to their published Windows desktop and applications. This client could either be a native application on the device or the Windows Virtual Desktop HTML5 web client.
You can make sure your session host virtual machines (VMs) run near apps and services that connect to your datacenter or the cloud. This way your users stay productive and don't encounter long load times.
User sign-in to Windows Virtual Desktop is fast because user profiles are containerized by using FSLogix. At sign-in, the user profile container is dynamically attached to the computing environment. The user profile is immediately available and appears in the system exactly like a native user profile.
You can provide individual ownership through personal (persistent) desktops. For example, you might want to provide personal remote desktops for members of an engineering team. Then they can add or remove programs without impacting other users on that remote desktop.

Enhance security

Windows Virtual Desktop provides centralized security management for users' desktops with Azure Active Directory (Azure AD). You can enable multifactor authentication to secure user sign-ins. You can also secure access to data by assigning granular role-based access controls (RBACs) to users.
With Windows Virtual Desktop, the data and apps are separated from the local hardware. Windows Virtual Desktop runs them instead on a remote server. The risk of confidential data being left on a personal device is reduced.
User sessions are isolated in both single and multi-session environments.
Windows Virtual Desktop also improves security by using reverse connect technology. This connection type is more secure than the Remote Desktop Protocol. We don't open inbound ports to the session host VMs.

What are some key features of Windows Virtual Desktop?

Simplified management

Windows Virtual Desktop is an Azure service, so it will be familiar to Azure administrators. You use Azure AD and RBACs to manage access to resources. With Azure, you also get tools to automate VM deployments, manage VM updates, and provide disaster recovery. As with other Azure services, Windows Virtual Desktop uses Azure Monitor for monitoring and alerts. This standardization lets admins identify issues through a single interface.

Performance management

Windows Virtual Desktop gives you options to load balance users on your VM host pools. *Host pools* are collections of VMs with the same configuration assigned to multiple users. For the best performance, you can configure load balancing to occur as users sign in (breadth mode). With breadth mode, users are sequentially allocated across the host pool for your workload. To save costs, you can configure your VMs for depth mode load balancing where users are fully allocated on one VM before moving to the next. Windows Virtual Desktop provides tools to automatically provision additional VMs when incoming demand exceeds a specified threshold.

Multi-session Windows 10 deployment

Windows Virtual Desktop lets you use Windows 10 Enterprise multi-session, the only Windows client-based operating system that enables multiple concurrent users on a single VM. Windows Virtual Desktop also provides a more consistent experience with broader application support compared to Windows Server-based operating systems.

How can you reduce costs with Windows Virtual Desktop?

Bring your own licenses

Windows Virtual Desktop is available to you at no additional cost if you have an eligible Microsoft 365 license. Just pay for the Azure resources used by Windows Virtual Desktop.

- Bring your eligible Windows or Microsoft 365 license to get Windows 10 Enterprise and Windows 7 Enterprise desktops and apps at no additional cost.
- If you're an eligible Microsoft Remote Desktop Services Client Access License customer, Windows Server Remote Desktop Services desktops and apps are available at no additional cost.

Save on compute costs

Buy one-year or three-year Azure Reserved Virtual Machine Instances to save you up to 72 percent versus pay-as-you-go pricing. You can pay for a reservation up front or monthly. Reservations provide a billing discount and don't affect the runtime state of your resources.

From <https://docs.microsoft.com/en-us/learn/modules/azure-compute-fundamentals/windows-virtual-desktop>

Explore Azure Storage services

Thursday, January 28, 2021 10:24 AM

In this module, you'll learn about some of the different storage options that are available in Azure Storage services, and the scenarios in which each storage option is appropriate. As you complete the individual units in this module, you'll learn about Azure Blob Storage, Azure Disk Storage, Azure Files, and Blob access tiers.

Overview

- Introduction 2 min
- Azure Storage account fundamentals 4 min
- Disk storage fundamentals 4 min
- Azure Blob storage fundamentals 4 min
- Azure Files fundamentals 4 min
- Understanding Blob access tiers 4 min
- Knowledge check 3 min
- Summary 2 min

From <https://docs.microsoft.com/en-us/learn/paths/az-900-describe-core-azure-services/>

Introduction

- 2 minutes

Suppose your company, Tailwind Traders, has a number of product brochures, datasheets, product images, and other files that are related to marketing, sales, and support. In the past, your company has been hosting these files on standalone web servers in your datacenter.

Your company is now in the process of migrating its applications to the cloud, and your development team is currently architecting new applications. Your Chief Technology Officer (CTO) wants to migrate all of your marketing, sales, and support files to the cloud in order to take advantage of geographic distribution of your files. This move also reduces the number of physical servers that your company maintains in your datacenter. As part of your migration strategy, you need to determine the correct approach for your cloud-based storage infrastructure.

In this module, you'll learn about the different Azure storage options and the scenarios in which each is appropriate.

Note

Azure storage isn't the same as Azure database services.

Learning objectives

After completing this module, you'll be able to describe the benefits and usage of:

- Azure Blob Storage
- Azure Disk Storage
- Azure Files Storage
- Azure Blob Access tiers

Prerequisites

- You should be familiar with basic computing concepts and terminology

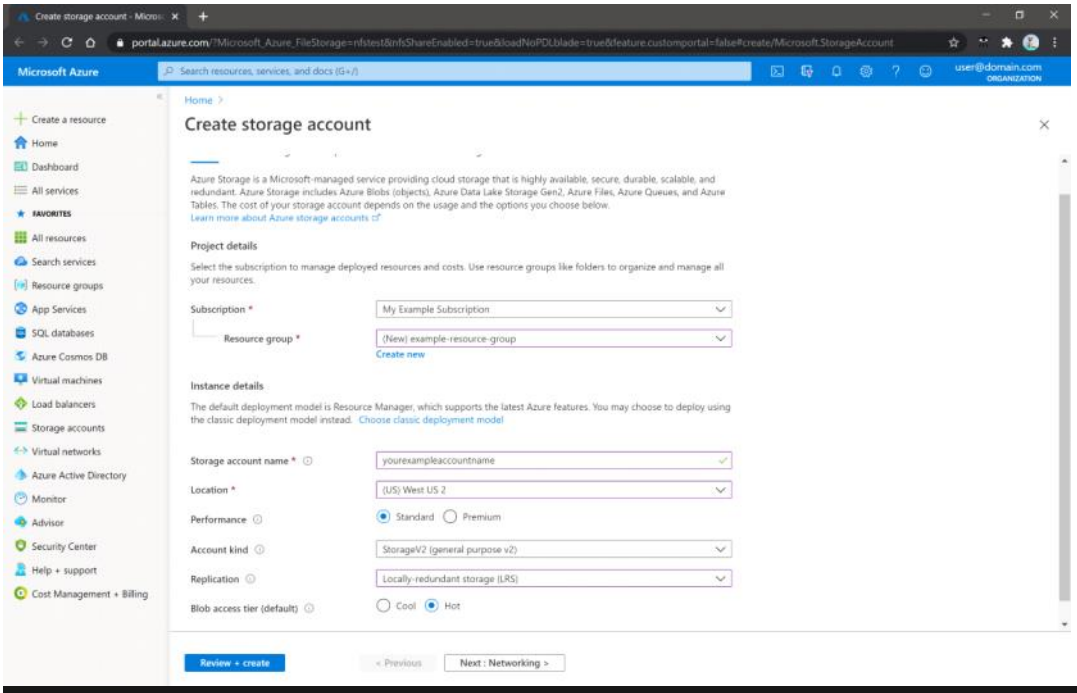
From <https://docs.microsoft.com/en-us/learn/modules/azure-storage-fundamentals/introduction>

Azure Storage account fundamentals

- 4 minutes

The Chief Technology Officer (CTO) for your company, Tailwind Traders, has tasked your team with migrating all of your files to the cloud. Your team has chosen Azure Storage , which is a service that you can use to store files, messages, tables, and other types of information. Clients such as websites, mobile apps, desktop applications, and many other types of custom solutions can read data from and write data to Azure Storage. Azure Storage is also used by infrastructure as a service virtual machines, and platform as a service cloud services.

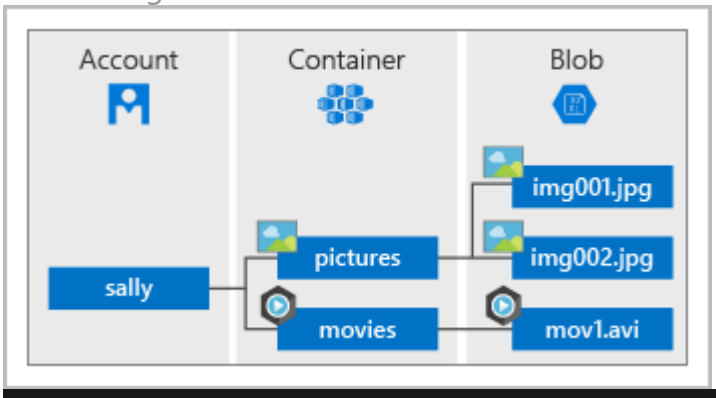
To begin using Azure Storage, you first create an Azure Storage account to store your data objects. You can create an Azure Storage account by using the Azure portal, PowerShell, or the Azure CLI.



Your storage account will contain all of your Azure Storage data objects, such as blobs, files, and disks.

Note

Azure VMs use Azure Disk Storage to store virtual disks. However, you can't use Azure Disk Storage to store a disk outside of a virtual machine.



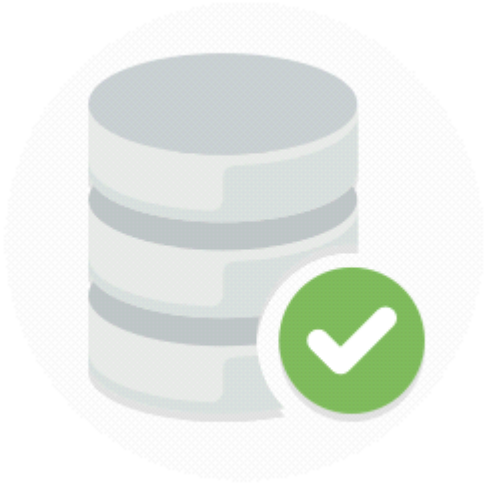
A storage account provides a unique namespace for your Azure Storage data, that's accessible from anywhere in the world over HTTP or HTTPS. Data in this account is secure, highly available, durable, and massively scalable.
For more information, see Create a storage account .

From <https://docs.microsoft.com/en-us/learn/modules/azure-storage-fundamentals/azure-storage-accounts>

Disk storage fundamentals

- 4 minutes

Disk Storage provides disks for Azure virtual machines. Applications and other services can access and use these disks as needed, similar to how they would in on-premises scenarios. Disk Storage allows data to be persistently stored and accessed from an attached virtual hard disk.



Disks come in many different sizes and performance levels, from solid-state drives (SSDs) to traditional spinning hard disk drives (HDDs), with varying performance tiers. You can use standard SSD and HDD disks for less critical workloads, premium SSD disks for mission-critical production applications, and ultra disks for data-intensive workloads such as SAP HANA, top tier databases, and transaction-heavy workloads. Azure has consistently delivered enterprise-grade durability for infrastructure as a service (Iaas) disks, with an industry-leading ZERO% annualized failure rate.
The following illustration shows an Azure virtual machine that uses separate disks to store different data.

From <https://docs.microsoft.com/en-us/learn/modules/azure-storage-fundamentals/azure-disk-storage>

Azure Blob storage fundamentals

- 4 minutes

Azure Blob Storage is an object storage solution for the cloud. It can store massive amounts of data, such as text or binary data. Azure Blob Storage is unstructured, meaning that there are no restrictions on the kinds of data it can hold. Blob Storage can manage thousands of simultaneous uploads, massive amounts of video data, constantly growing log files, and can be reached from anywhere with an internet connection.

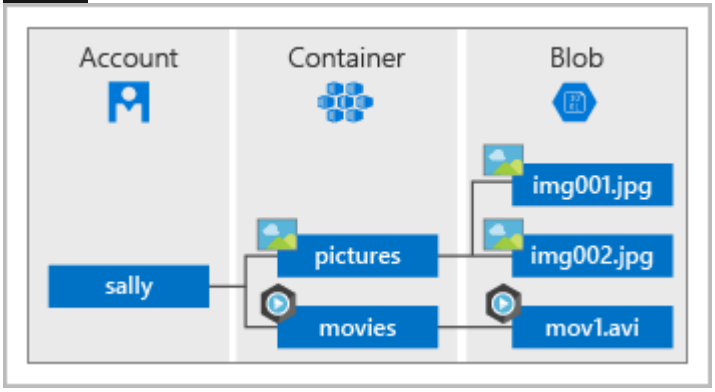
Blobs aren't limited to common file formats. A blob could contain gigabytes of binary data streamed from a scientific instrument, an encrypted message for another application, or data in a custom format for an app you're developing. One advantage of blob storage over disk storage is that it does not require developers to think about or manage disks; data is uploaded as blobs, and Azure takes care of the physical storage needs.

Blob Storage is ideal for:

- Serving images or documents directly to a browser.
- Storing files for distributed access.
- Streaming video and audio.
- Storing data for backup and restore, disaster recovery, and archiving.
- Storing data for analysis by an on-premises or Azure-hosted service.
- Storing up to 8 TB of data for virtual machines.

You store blobs in containers, which helps you organize your blobs depending on your business needs.

The following diagram illustrates how you might use Azure accounts, containers, and blobs.



From <https://docs.microsoft.com/en-us/learn/modules/azure-storage-fundamentals/azure-blob-container-storage>

Azure Files fundamentals

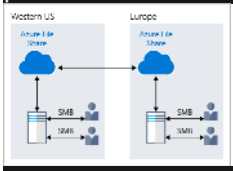
- 4 minutes

Azure Files offers fully managed file shares in the cloud that are accessible via the industry standard Server Message Block and Network File System (preview) protocols. Azure file shares can be mounted concurrently by cloud or on-premises deployments of Windows, Linux, and macOS. Applications running in Azure virtual machines or cloud services can mount a file storage share to access file data, just as a desktop application would mount a typical SMB share. Any number of Azure virtual machines or roles can mount and access the file storage share simultaneously. Typical usage scenarios would be to share files anywhere in the world, diagnostic data, or application data sharing.

Use Azure Files for the following situations:

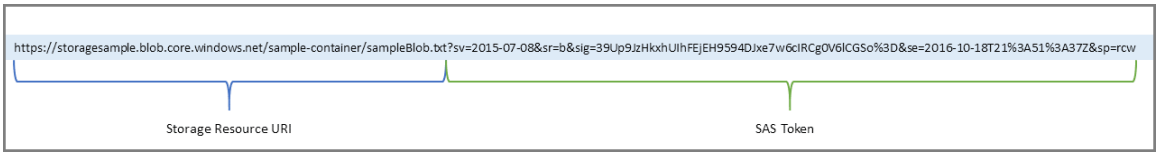
- Many on-premises applications use file shares. Azure Files makes it easier to migrate those applications that share data to Azure. If you mount the Azure file share to the same drive letter that the on-premises application uses, the part of your application that accesses the file share should work with minimal, if any, changes.
- Store configuration files on a file share and access them from multiple VMs. Tools and utilities used by multiple developers in a group can be stored on a file share, ensuring that everybody can find them, and that they use the same version.
- Write data to a file share, and process or analyze the data later. For example, you might want to do this with diagnostic logs, metrics, and crash dumps.

The following illustration shows Azure Files being used to share data between two geographical locations. Azure Files ensures the data is encrypted at rest, and the SMB protocol ensures the data is encrypted in transit.



One thing that distinguishes Azure Files from files on a corporate file share is that you can access the files from anywhere in the world, by using a URL that points to the file. You can also use Shared Access Signature (SAS) tokens to allow access to a private asset for a specific amount of time.

Here's an example of a service SAS URI, showing the resource URI and the SAS token:



From <https://docs.microsoft.com/en-us/learn/modules/azure-storage-fundamentals/azure-file-storage>

Understanding Blob access tiers

- 4 minutes

Data stored in the cloud can grow at an exponential pace. To manage costs for your expanding storage needs, it's helpful to organize your data based on attributes like frequency of access and planned retention period. Data stored in the cloud can be different based on how it's generated, processed, and accessed over its lifetime. Some data is actively accessed and modified throughout its lifetime. Some data is accessed frequently early in its lifetime, with access dropping drastically as the data ages. Some data remains idle in the cloud and is rarely, if ever, accessed after it's stored. To accommodate these different access needs, Azure provides several *access tiers*, which you can use to balance your storage costs with your access needs.

Azure Storage offers different access tiers for your blob storage, helping you store object data in the most cost-effective manner. The available access tiers include:

- Hot access tier: Optimized for storing data that is accessed frequently (for example, images for your website).
- Cool access tier: Optimized for data that is infrequently accessed and stored for at least 30 days (for example, invoices for your customers).
- Archive access tier: Appropriate for data that is rarely accessed and stored for at least 180 days, with flexible latency requirements (for example, long-term backups).

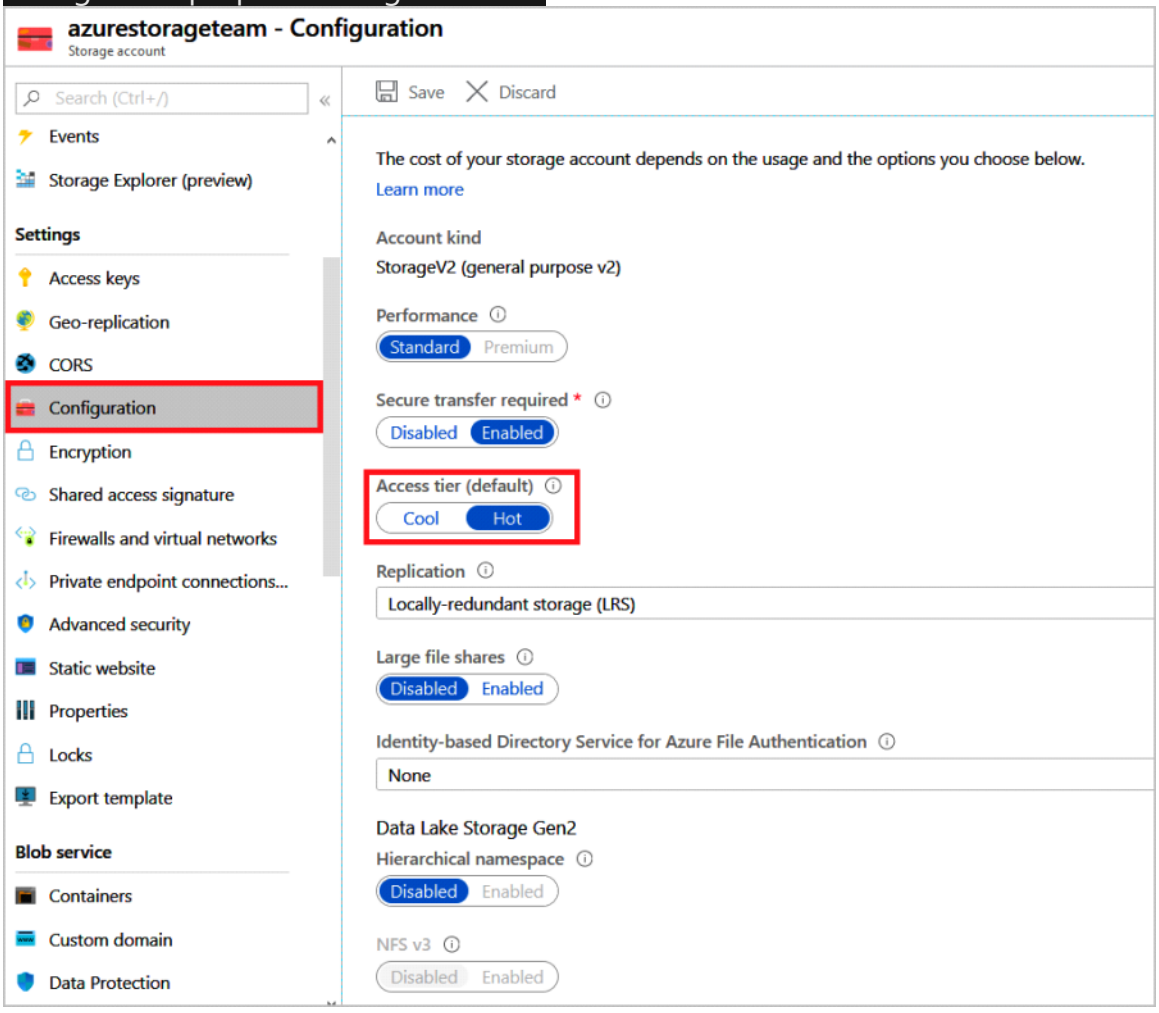
The following considerations apply to the different access tiers:

- Only the hot and cool access tiers can be set at the account level. The archive access tier isn't available at the account level.
- Hot, cool, and archive tiers can be set at the blob level, during upload or after upload.
- Data in the cool access tier can tolerate slightly lower availability, but still requires high durability, retrieval latency, and throughput characteristics similar to hot data. For cool data, a slightly lower availability service-level agreement (SLA) and higher

access costs compared to hot data are acceptable trade-offs for lower storage costs.

- Archive storage stores data offline and offers the lowest storage costs, but also the highest costs to rehydrate and access data.

The following illustration demonstrates choosing between the hot and cool access tiers on a general purpose storage account.



From <https://docs.microsoft.com/en-us/learn/modules/azure-storage-fundamentals/azure-storage-tiers>

Explore Azure networking services

Thursday, January 28, 2021 10:26 AM

In this module, you'll take a look at several of the core networking resources that are available in Azure. You'll learn about Azure Virtual Network, which you can configure into a customized network environment that meets your company's needs. You'll also learn how you can use Azure VPN Gateway and Azure ExpressRoute to create secure communication tunnels between your company's different locations.

Overview

- Introduction 2 min
- Azure Virtual Network fundamentals 8 min
- Azure Virtual Network settings 7 min
- Azure VPN Gateway fundamentals 10 min
- Azure ExpressRoute fundamentals 5 min
- Knowledge check 4 min
- Summary 2 min

From <https://docs.microsoft.com/en-us/learn/paths/az-900-describe-core-azure-services/>

Introduction

- 2 minutes

Suppose your company, Tailwind Traders, has migrated some applications to the cloud and is architecting new ones. The servers that host Tailwind Traders' customer and product data are based in Silicon Valley. Your company also has several branch offices located in different geographic regions. As part of your migration strategy, your company needs to determine the correct approach to configure its network infrastructure.

To help save costs, you convince your team to move your website and several of your other networked resources to the cloud. With that in mind, you'll need to provide secure access to private company data for each of its branch locations. You want to know how Azure can help you manage your network more effectively. As it turns out, managing networks on Azure isn't entirely different from managing on-premises networks.
In this module, you'll learn about the different Azure networking options and the scenarios in which each is appropriate.

Learning objectives

After completing this module, you'll be able to:

- Describe the core networking resources that are available in Azure.
- Describe the benefits and usage of Azure Virtual Network, Azure VPN Gateway, and Azure ExpressRoute.

Prerequisites

- You should be familiar with basic network concepts and terminology.
- Familiarity with cloud computing is helpful but isn't necessary.

From <https://docs.microsoft.com/en-us/learn/modules/azure-networking-fundamentals/introduction>

Azure Virtual Network fundamentals

- 8 minutes

Tailwind Traders has an on-premises datacenter that you plan to keep, but you want to use Azure to offload peak traffic by using virtual machines (VMs) hosted in Azure. You want to keep your existing IP addressing scheme and network appliances while ensuring that any data transfer is secure.

Using Azure Virtual Network for your virtual networking can help you reach your goals.

What is Azure virtual networking?

Azure virtual networks enable Azure resources, such as VMs, web apps, and databases, to communicate with each other, with users on the internet, and with your on-premises client computers. You can think of an Azure network as a set of resources that links other Azure resources.

Azure virtual networks provide the following key networking capabilities:

- Isolation and segmentation
- Internet communications
- Communicate between Azure resources
- Communicate with on-premises resources
- Route network traffic
- Filter network traffic
- Connect virtual networks

Network configurations for virtual machines

Isolation and segmentation

Virtual Network allows you to create multiple isolated virtual networks. When you set up a virtual network, you define a private IP address space by using either public or private IP address ranges. You can divide that IP address space into subnets and allocate part of the defined address space to each named subnet.
For name resolution, you can use the name resolution service that's built in to Azure. You also can configure the virtual network to use either an internal or an external DNS server.

Internet communications

A VM in Azure can connect to the internet by default. You can enable incoming connections from the internet by defining a public IP address or a public load balancer. For VM management, you can connect via the Azure CLI, Remote Desktop Protocol, or Secure Shell.

Communicate between Azure resources

You'll want to enable Azure resources to communicate securely with each other. You can do that in one of two ways:

- Virtual networks
  Virtual networks can connect not only VMs but other Azure resources, such as the App Service Environment for Power Apps, Azure Kubernetes Service, and Azure virtual machine scale sets.
- Service endpoints
  You can use service endpoints to connect to other Azure resource types, such as Azure SQL databases and storage accounts. This approach enables you to link multiple Azure resources to virtual networks to improve security and provide optimal routing between resources.

Communicate with on-premises resources

Azure virtual networks enable you to link resources together in your on-premises environment and within your Azure subscription. In effect, you can create a network that spans both your local and cloud environments. There are three mechanisms for you to achieve this connectivity:

- Point-to-site virtual private networks
  This approach is like a virtual private network (VPN) connection that a computer outside your organization makes back into your corporate network, except that it's working in the opposite direction. In this case, the client computer initiates an encrypted VPN connection to Azure to connect that computer to the Azure virtual network.
- Site-to-site virtual private networks
  A site-to-site VPN links your on-premises VPN device or gateway to the Azure VPN

gateway in a virtual network. In effect, the devices in Azure can appear as being on the local network. The connection is encrypted and works over the internet.

- Azure ExpressRoute
  For environments where you need greater bandwidth and even higher levels of security, Azure ExpressRoute is the best approach. ExpressRoute provides dedicated private connectivity to Azure that doesn't travel over the internet. (You'll learn more about ExpressRoute in a separate unit later in this module.)

Route network traffic

By default, Azure routes traffic between subnets on any connected virtual networks, on-premises networks, and the internet. You also can control routing and override those settings, as follows:

- Route tables
  A route table allows you to define rules about how traffic should be directed. You can create custom route tables that control how packets are routed between subnets.
- Border Gateway Protocol
  Border Gateway Protocol (BGP) works with Azure VPN gateways or ExpressRoute to propagate on-premises BGP routes to Azure virtual networks.

Filter network traffic

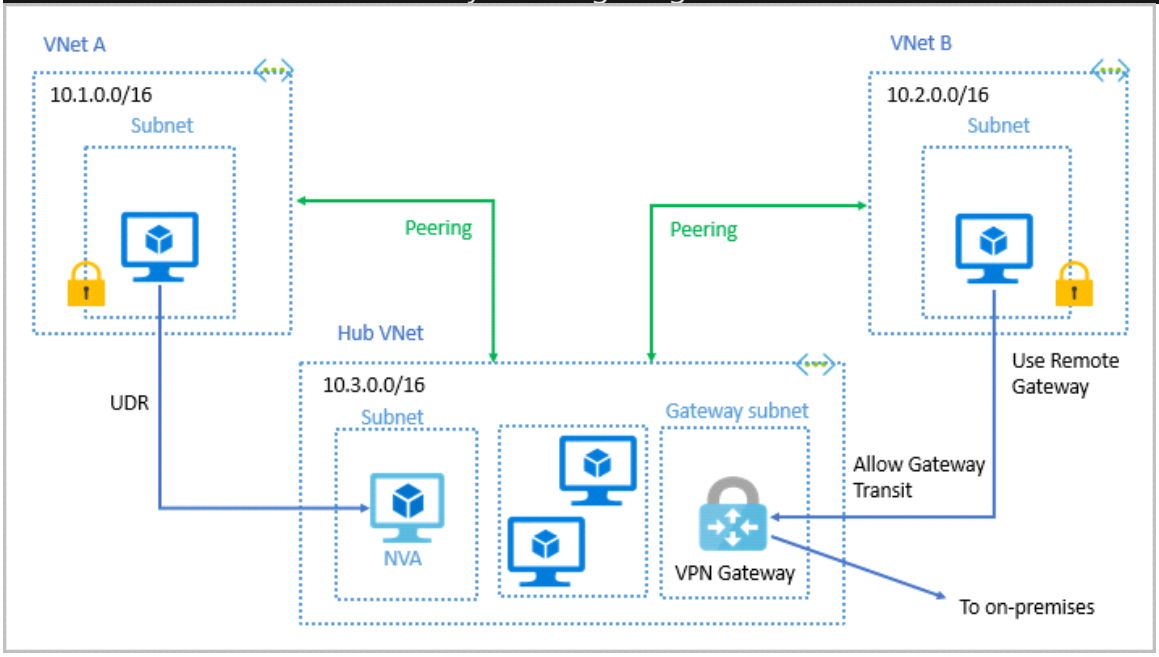
Azure virtual networks enable you to filter traffic between subnets by using the following approaches:

- Network security groups
  A network security group is an Azure resource that can contain multiple inbound and outbound security rules. You can define these rules to allow or block traffic, based on factors such as source and destination IP address, port, and protocol.
- Network virtual appliances
  A network virtual appliance is a specialized VM that can be compared to a hardened network appliance. A network virtual appliance carries out a particular network function, such as running a firewall or performing wide area network (WAN) optimization.

Connect virtual networks

You can link virtual networks together by using virtual network *peering*. Peering enables resources in each virtual network to communicate with each other. These virtual networks can be in separate regions, which allows you to create a global interconnected network through Azure.
UDR is user-defined Routing. UDR is a significant update to Azure’s Virtual Networks as this allows network admins to control the routing tables between subnets within a VNet,

as well as between VNets, thereby allowing for greater control over network traffic flow.



From <https://docs.microsoft.com/en-us/learn/modules/azure-networking-fundamentals/azure-virtual-network-fundamentals>

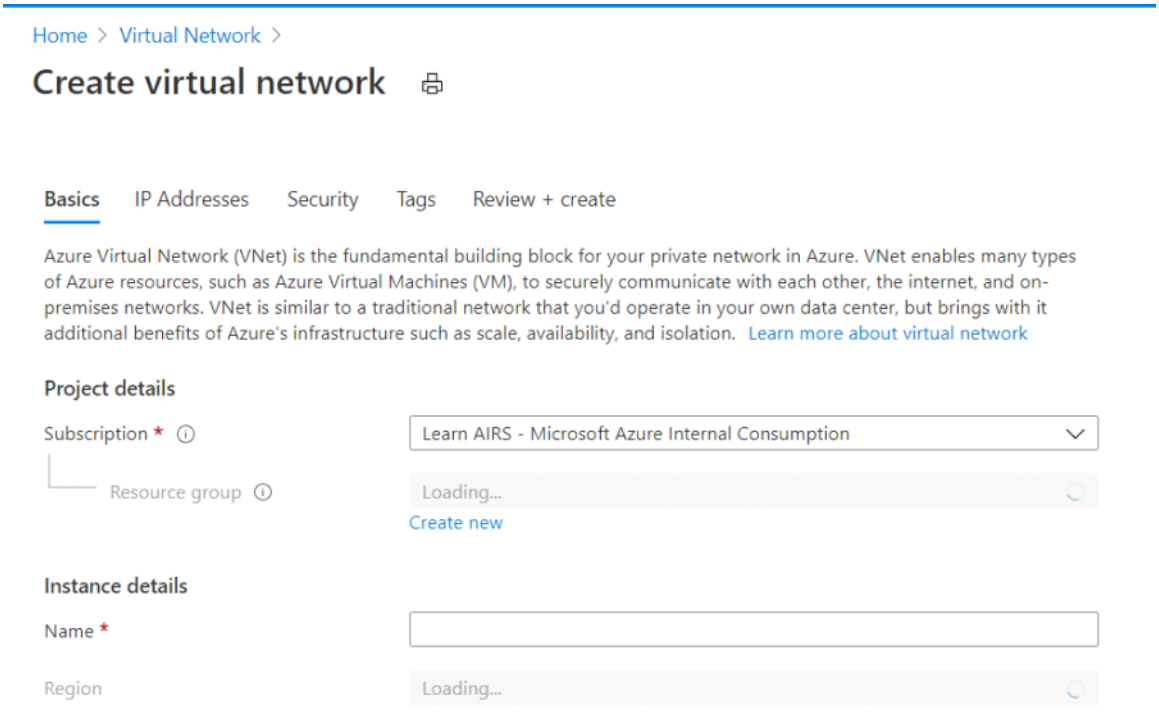
Azure Virtual Network settings

- 7 minutes

You can create and configure Azure Virtual Network instances from the Azure portal, Azure PowerShell on your local computer, or Azure Cloud Shell.

Create a virtual network

When you create an Azure virtual network, you configure a number of basic settings. You'll have the option to configure advanced settings, such as multiple subnets, distributed denial of service (DDoS) protection, and service endpoints.



You'll configure the following settings for a basic virtual network:

- Network name
  The network name must be unique in your subscription, but it doesn't need to be globally unique. Make the name a descriptive one that's easy to remember and identified from other virtual networks.
- Address space
  When you set up a virtual network, you define the internal address space in Classless Interdomain Routing (CIDR) format. This address space needs to be unique within your subscription and any other networks that you connect to. Let's assume you choose an address space of 10.0.0.0/24 for your first virtual network. The addresses defined in this address space range from 10.0.0.1 to 10.0.0.254. You then create a second virtual network and choose an address space of 10.0.0.0/8. The addresses in this address space range from 10.0.0.1 to 10.255.255.254. Some of the addresses overlap and can't be used for the two virtual networks.
  But you can use 10.0.0.0/16, with addresses that range from 10.0.0.1 to 10.0.255.254, and 10.1.0.0/16, with addresses that range from 10.1.0.1 to 10.1.255.254. You can assign these address spaces to your virtual networks because there's no address overlap.
  Note
  You can add address spaces after you create the virtual network.
- Subscription
  This option only applies if you have multiple subscriptions to choose from.
- Resource group
  Like any other Azure resource, a virtual network needs to exist in a resource group.

You can either select an existing resource group or create a new one.

- Location
  Select the location where you want the virtual network to exist.
- Subnet
  Within each virtual network address range, you can create one or more subnets that partition the virtual network's address space. Routing between subnets will then depend on the default traffic routes. You also can define custom routes. Alternatively, you can define one subnet that encompasses all the virtual networks' address ranges.
  Note
  Subnet names must begin with a letter or number and end with a letter, number, or underscore. They may contain only letters, numbers, underscores, periods, or hyphens.
- DDoS protection
  You can select either Basic or Standard DDoS protection. Standard DDoS protection is a premium service. For more information on Standard DDoS protection, see Azure DDoS protection Standard overview .
- Service endpoints
  Here, you enable service endpoints. Then you select from the list which Azure service endpoints you want to enable. Options include Azure Cosmos DB, Azure Service Bus, Azure Key Vault, and so on.

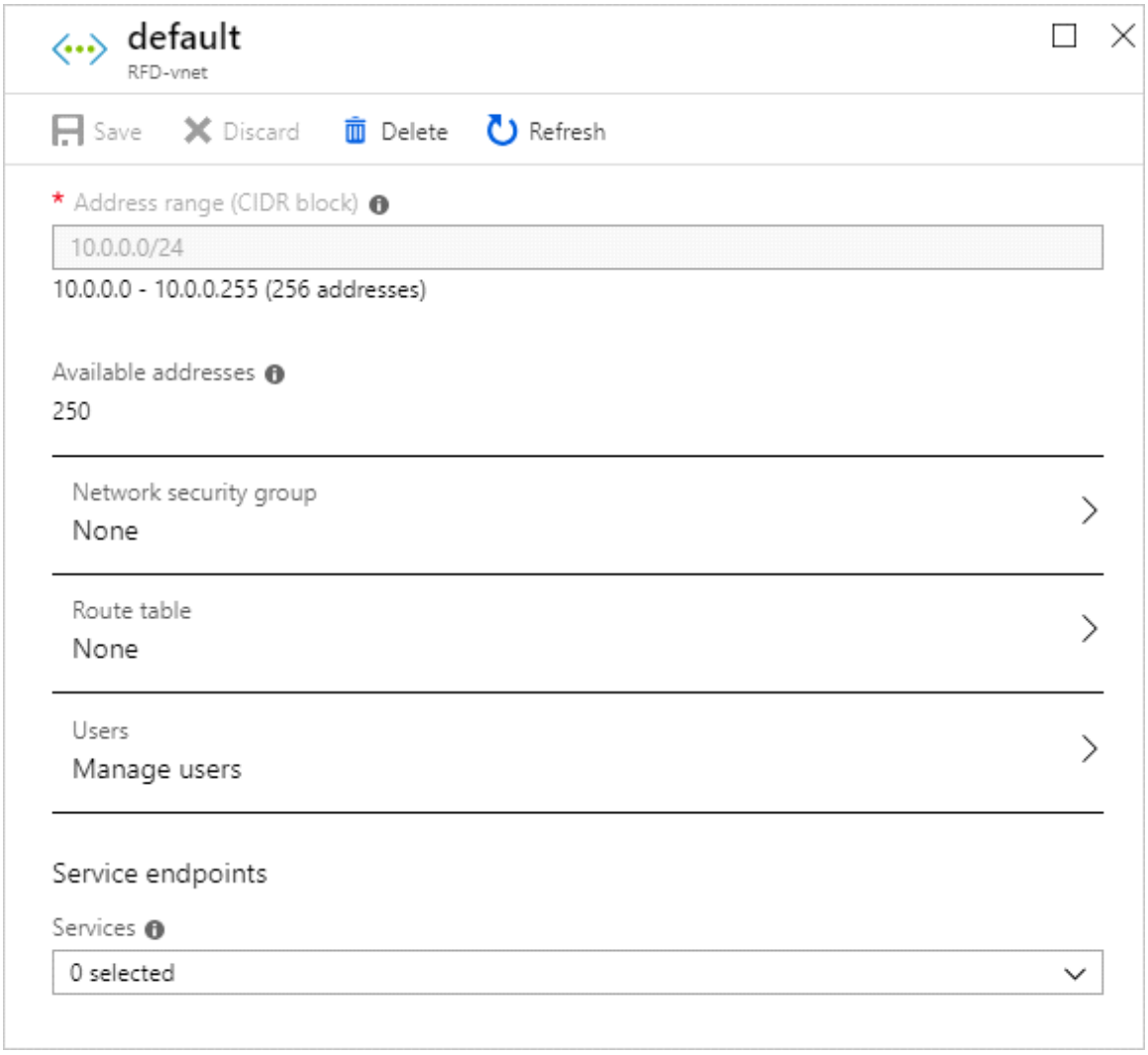
After you've configured these settings, select Create.

Define additional settings

After you create a virtual network, you can then define further settings. These include:

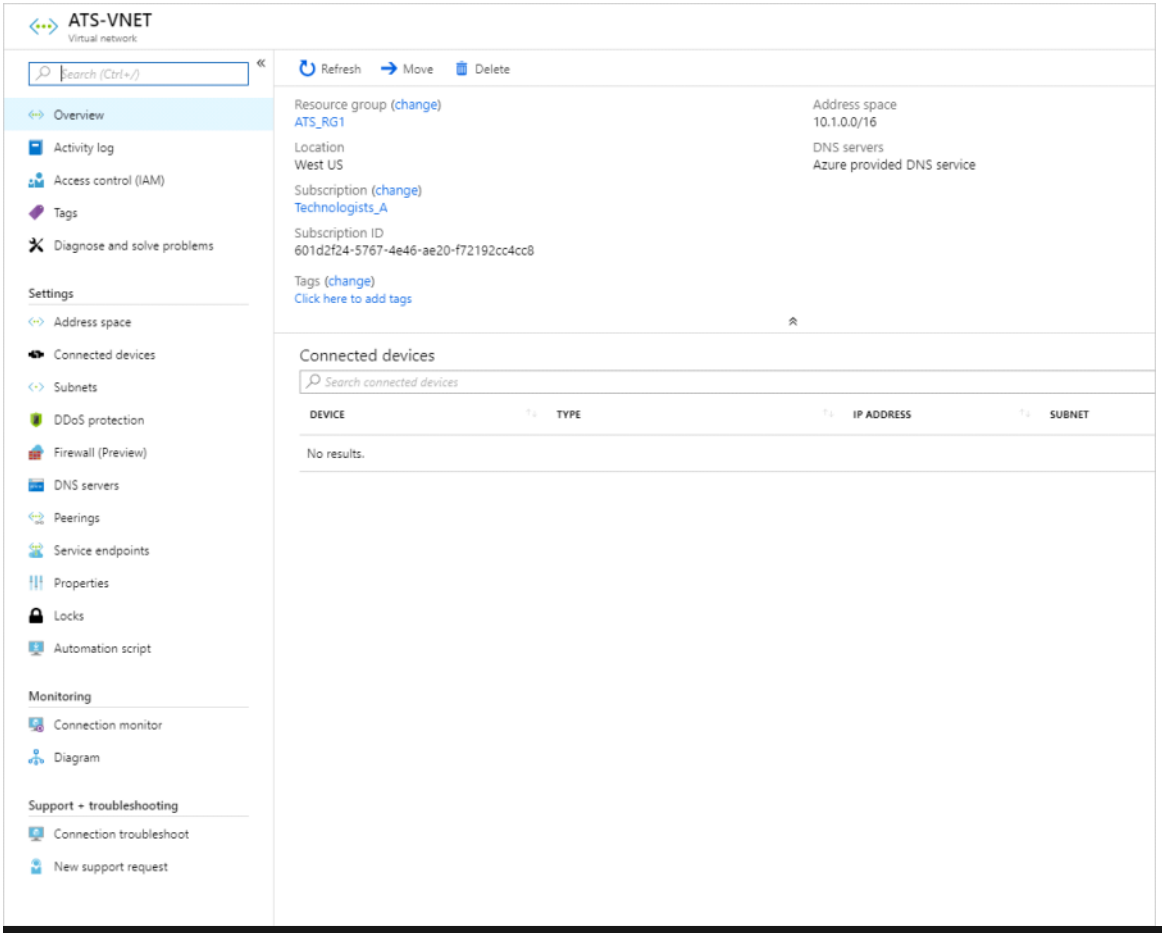
- Network security group
  Network security groups have security rules that enable you to filter the type of network traffic that can flow in and out of virtual network subnets and network interfaces. You create the network security group separately. Then you associate it with the virtual network.
- Route table
  Azure automatically creates a route table for each subnet within an Azure virtual network and adds system default routes to the table. You can add custom route tables to modify traffic between virtual networks.

You can also amend the service endpoints.



Configure virtual networks

After you've created a virtual network, you can change any further settings on the Virtual network pane in the Azure portal. Alternatively, you can use PowerShell commands or commands in Cloud Shell to make changes.



You can then review and change settings in further subpanes. These settings include:

- Address spaces: You can add additional address spaces to the initial definition.
- Connected devices: Use the virtual network to connect machines.
- Subnets: You can add additional subnets.
- Peerings: Link virtual networks in peering arrangements.

You can also monitor and troubleshoot virtual networks. Or, you can create an automation script to generate the current virtual network.

Virtual networks are powerful and highly configurable mechanisms for connecting entities in Azure. You can connect Azure resources to one another or to resources you have on-premises. You can isolate, filter, and route your network traffic. Azure allows you to increase security where you feel you need it.

From <https://docs.microsoft.com/en-us/learn/modules/azure-networking-fundamentals/azure-virtual-network-settings>

Azure VPN Gateway fundamentals

- 10 minutes

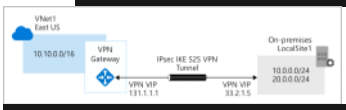
A virtual private network (VPN) is a type of private interconnected network. VPNs use an encrypted tunnel within another network. They're typically deployed to connect two or more trusted private networks to one another over an untrusted network (typically the public internet). Traffic is encrypted while traveling over the untrusted network to prevent eavesdropping or other attacks.

For our Tailwind Traders scenario, VPNs can enable branch offices to share sensitive information between locations. For example, let's say that your offices on the East Coast region of North America need to access your company's private customer data, which is stored on servers that are physically located in a West Coast region. A VPN that connects your East Coast offices to your West Coast servers allows your company to securely access your private customer data.

VPN gateways

A VPN gateway is a type of virtual network gateway. Azure VPN Gateway instances are deployed in Azure Virtual Network instances and enable the following connectivity:

- Connect on-premises datacenters to virtual networks through a *site-to-site* connection.
- Connect individual devices to virtual networks through a *point-to-site* connection.
- Connect virtual networks to other virtual networks through a *network-to-network* connection.



All transferred data is encrypted in a private tunnel as it crosses the internet. You can deploy only one VPN gateway in each virtual network, but you can use one gateway to connect to multiple locations, which includes other virtual networks or on-premises datacenters.

When you deploy a VPN gateway, you specify the VPN type: either *policy-based* or *route-based*. The main difference between these two types of VPNs is how traffic to be encrypted is specified. In Azure, both types of VPN gateways use a pre-shared key as the only method of authentication. Both types also rely on Internet Key Exchange (IKE) in either version 1 or version 2 and Internet Protocol Security (IPSec). IKE is used to set up a security association (an agreement of the encryption) between two endpoints. This association is then passed to the IPSec suite, which encrypts and decrypts data packets encapsulated in the VPN tunnel.

Policy-based VPNs

Policy-based VPN gateways specify statically the IP address of packets that should be encrypted through each tunnel. This type of device evaluates every data packet against those sets of IP addresses to choose the tunnel where that packet is going to be sent through.

Key features of policy-based VPN gateways in Azure include:

- Support for IKEv1 only.
- Use of *static routing*, where combinations of address prefixes from both networks control how traffic is encrypted and decrypted through the VPN tunnel. The source and destination of the tunneled networks are declared in the policy and don't need to be declared in routing tables.

- Policy-based VPNs must be used in specific scenarios that require them, such as for compatibility with legacy on-premises VPN devices.

Route-based VPNs

If defining which IP addresses are behind each tunnel is too cumbersome, route-based gateways can be used. With route-based gateways, IPSec tunnels are modeled as a network interface or virtual tunnel interface. IP routing (either static routes or dynamic routing protocols) decides which one of these tunnel interfaces to use when sending each packet. Route-based VPNs are the preferred connection method for on-premises devices. They're more resilient to topology changes such as the creation of new subnets.
Use a route-based VPN gateway if you need any of the following types of connectivity:

- Connections between virtual networks
- Point-to-site connections
- Multisite connections
- Coexistence with an Azure ExpressRoute gateway

Key features of route-based VPN gateways in Azure include:

- Supports IKEv2
- Uses any-to-any (wildcard) traffic selectors
- Can use *dynamic routing protocols*, where routing/forwarding tables direct traffic to different IPSec tunnels
  In this case, the source and destination networks aren't statically defined as they are in policy-based VPNs or even in route-based VPNs with static routing. Instead, data packets are encrypted based on network routing tables that are created dynamically using routing protocols such as Border Gateway Protocol (BGP).

VPN gateway sizes

The capabilities of your VPN gateway are determined by the SKU or size that you deploy. This table shows the main capabilities of each available SKU.

SKU	Site-to-site/Network-to-network tunnels	Aggregate throughput benchmark	Border Gateway Protocol support
Basic [See Note]	Maximum: 10	100 Mbps	Not supported
VpnGw1/Az	Maximum: 30	650 Mbps	Supported
VpnGw2/Az	Maximum: 30	1 Gbps	Supported
VpnGw3/Az	Maximum: 30	1.25 Gbps	Supported

VPN GATEWAY SIZES

Note

A Basic VPN gateway should only be used for Dev/Test workloads. In addition, it's unsupported to migrate from Basic to the VpnGW1/2/3/Az SKUs at a later time without having to remove the gateway and redeploy.

Deploy VPN gateways

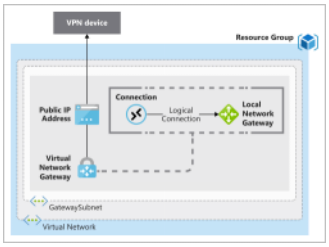
Before you can deploy a VPN gateway, you'll need some Azure and on-premises resources.

Required Azure resources

You'll need these Azure resources before you can deploy an operational VPN gateway:

- Virtual network. Deploy a virtual network with enough address space for the additional subnet that you'll need for the VPN gateway. The address space for this virtual network must not overlap with the on-premises network that you'll be connecting to. You can deploy only one VPN gateway within a virtual network.
- GatewaySubnet. Deploy a subnet called GatewaySubnet for the VPN gateway. Use at least a /27 address mask to make sure you have enough IP addresses in the subnet for future growth. You can't use this subnet for any other services.
- Public IP address. Create a Basic-SKU dynamic public IP address if you're using a non-zone-aware gateway. This address provides a public-routable IP address as the target for your on-premises VPN device. This IP address is dynamic, but it won't change unless you delete and re-create the VPN gateway.
- Local network gateway. Create a local network gateway to define the on-premises network's configuration, such as where the VPN gateway will connect and what it will connect to. This configuration includes the on-premises VPN device's public IPv4 address and the on-premises routable networks. This information is used by the VPN gateway to route packets that are destined for on-premises networks through the IPSec tunnel.
- Virtual network gateway. Create the virtual network gateway to route traffic between the virtual network and the on-premises datacenter or other virtual networks. The virtual network gateway can be either a VPN or ExpressRoute gateway, but this unit only deals with VPN virtual network gateways. (You'll learn more about ExpressRoute in a separate unit later in this module.)
- Connection. Create a connection resource to create a logical connection between the VPN gateway and the local network gateway.
- The connection is made to the on-premises VPN device's IPv4 address as defined by the local network gateway.
- The connection is made from the virtual network gateway and its associated public IP address.
  You can create multiple connections.

The following diagram shows this combination of resources and their relationships to help you better understand what's required to deploy a VPN gateway.



Required on-premises resources

To connect your datacenter to a VPN gateway, you'll need these on-premises resources:

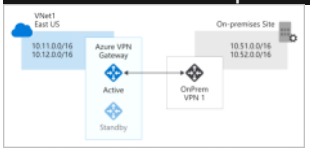
- A VPN device that supports policy-based or route-based VPN gateways
- A public-facing (internet-routable) IPv4 address

High-availability scenarios

There are several ways to ensure you have a fault-tolerant configuration.

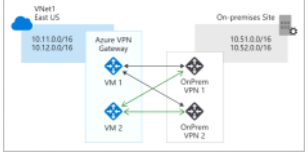
Active/standby

By default, VPN gateways are deployed as two instances in an active/standby configuration, even if you only see one VPN gateway resource in Azure. When planned maintenance or unplanned disruption affects the active instance, the standby instance automatically assumes responsibility for connections without any user intervention. Connections are interrupted during this failover, but they're typically restored within a few seconds for planned maintenance and within 90 seconds for unplanned disruptions.



Active/active

With the introduction of support for the BGP routing protocol, you can also deploy VPN gateways in an active/active configuration. In this configuration, you assign a unique public IP address to each instance. You then create separate tunnels from the on-premises device to each IP address. You can extend the high availability by deploying an additional VPN device on-premises.



ExpressRoute failover

Another high-availability option is to configure a VPN gateway as a secure failover path for ExpressRoute connections. ExpressRoute circuits have resiliency built in. But they aren't immune to physical problems that affect the cables delivering connectivity or outages that affect the complete ExpressRoute location. In high-availability scenarios, where there's risk associated with an outage of an ExpressRoute circuit, you can also provision a VPN gateway that uses the internet as an alternative method of connectivity. In this way, you can ensure there's always a connection to the virtual networks.

Zone-redundant gateways

In regions that support availability zones, VPN gateways and ExpressRoute gateways can be deployed in a zone-redundant configuration. This configuration brings resiliency, scalability, and higher availability to virtual network gateways. Deploying gateways in Azure availability zones physically and logically separates gateways within a region while protecting your on-premises network connectivity to Azure from zone-level failures. These gateways require different gateway SKUs and use Standard public IP addresses instead of Basic public IP addresses.

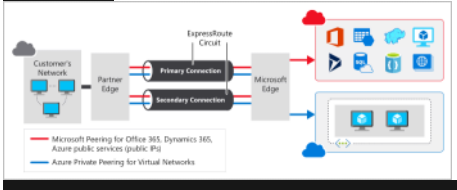
From <https://docs.microsoft.com/en-us/learn/modules/azure-networking-fundamentals/azure-vpn-gateway-fundamentals>

Azure ExpressRoute fundamentals

- 5 minutes

ExpressRoute lets you extend your on-premises networks into the Microsoft cloud over a private connection with the help of a connectivity provider. With ExpressRoute, you can establish connections to Microsoft cloud services, such as Microsoft Azure and Microsoft 365.

Connectivity can be from an any-to-any (IP VPN) network, a point-to-point Ethernet network, or a virtual cross-connection through a connectivity provider at a colocation facility. ExpressRoute connections don't go over the public Internet. This allows ExpressRoute connections to offer more reliability, faster speeds, consistent latencies, and higher security than typical connections over the Internet. For information on how to connect your network to Microsoft using ExpressRoute, see ExpressRoute connectivity models.



As part of your work for Tailwind Traders, you should understand what Azure ExpressRoute is and how it integrates with on-premises and Azure networks. In this unit, you'll learn about the benefits that ExpressRoute provides compared to other site-to-site connectivity options. As a result, you'll learn whether ExpressRoute can provide your company with the best possible network performance.

Throughout this unit, we'll focus on two different layers of the Open Systems Interconnection (OSI) model:

- Layer 2 (L2): This layer is the Data Link Layer, which provides node-to-node communication between two nodes on the same network.
- Layer 3 (L3): This layer is the Network Layer, which provides addressing and routing between nodes on a multi-node network.

Features and benefits of ExpressRoute

There are several benefits to using ExpressRoute as the connection service between Azure and on-premises networks.

- Layer 3 connectivity between your on-premises network and the Microsoft Cloud through a connectivity provider. Connectivity can be from an any-to-any (IPVPN) network, a point-to-point Ethernet connection, or through a virtual cross-connection via an Ethernet exchange.
- Connectivity to Microsoft cloud services across all regions in the geopolitical region.
- Global connectivity to Microsoft services across all regions with the ExpressRoute premium add-on.
- Dynamic routing between your network and Microsoft via BGP.
- Built-in redundancy in every peering location for higher reliability.
- Connection uptime SLA.
- QoS support for Skype for Business.

Layer 3 connectivity

ExpressRoute provides Layer 3 (address-level) connectivity between your on-premises network and the Microsoft cloud through connectivity partners. These connections can be from a point-to-point or any-to-any network. They can also be virtual cross-connections through an exchange.

Built-in redundancy

Each connectivity provider uses redundant devices to ensure that connections established with Microsoft are highly available. You can configure multiple circuits to complement this feature. All redundant connections are configured with Layer 3 connectivity to meet service-level agreements.

Connectivity to Microsoft cloud services

ExpressRoute enables direct access to the following services in all regions:

- Microsoft Office 365

- Microsoft Dynamics 365
- Azure compute services, such as Azure Virtual Machines
- Azure cloud services, such as Azure Cosmos DB and Azure Storage

Office 365 was created to be accessed securely and reliably via the internet. For this reason, we recommend the use of ExpressRoute for specific scenarios. The "Learn more" section at the end of this module includes a link about using ExpressRoute to access Office 365.

Across on-premises connectivity with ExpressRoute Global Reach

You can enable ExpressRoute Global Reach to exchange data across your on-premises sites by connecting your ExpressRoute circuits. For example, assume that you have a private datacenter in California connected to ExpressRoute in Silicon Valley. You have another private datacenter in Texas connected to ExpressRoute in Dallas. With ExpressRoute Global Reach, you can connect your private datacenters through two ExpressRoute circuits. Your cross-datacenter traffic will travel through the Microsoft network.

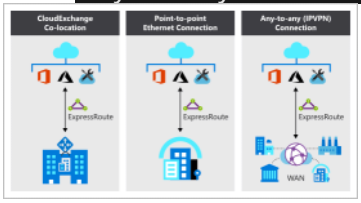
Dynamic routing

ExpressRoute uses the Border Gateway Protocol (BGP) routing protocol. BGP is used to exchange routes between on-premises networks and resources running in Azure. This protocol enables dynamic routing between your on-premises network and services running in the Microsoft cloud.

ExpressRoute connectivity models

ExpressRoute supports three models that you can use to connect your on-premises network to the Microsoft cloud:

- CloudExchange colocation
- Point-to-point Ethernet connection
- Any-to-any connection



Colocation at a cloud exchange

Colocated providers can normally offer both Layer 2 and Layer 3 connections between your infrastructure, which might be located in the colocation facility, and the Microsoft cloud. For example, if your datacenter is colocated at a cloud exchange such as an ISP,

you can request a virtual cross-connection to the Microsoft cloud.

Point-to-point Ethernet connection

Point-to-point connections provide Layer 2 and Layer 3 connectivity between your on-premises site and Azure. You can connect your offices or datacenters to Azure by using the point-to-point links. For example, if you have an on-premises datacenter, you can use a point-to-point Ethernet link to connect to Microsoft.

Any-to-any networks

With any-to-any connectivity, you can integrate your wide area network (WAN) with Azure by providing connections to your offices and datacenters. Azure integrates with your WAN connection to provide a connection like you would have between your datacenter and any branch offices.
With any-to-any connections, all WAN providers offer Layer 3 connectivity. For example, if you already use Multiprotocol Label Switching to connect to your branch offices or other sites in your organization, an ExpressRoute connection to Microsoft behaves like any other location on your private WAN.

Security considerations

With ExpressRoute, your data doesn't travel over the public internet, so it's not exposed to the potential risks associated with internet communications. ExpressRoute is a private connection from your on-premises infrastructure to your Azure infrastructure. Even if you have an ExpressRoute connection, DNS queries, certificate revocation list checking, and Azure Content Delivery Network requests are still sent over the public internet.

From <https://docs.microsoft.com/en-us/learn/modules/azure-networking-fundamentals/express-route-fundamentals>

Part 3: Describe core solutions and management tools on Azure

Thursday, January 28, 2021 10:29 AM

Choose the best AI service for your needs

Thursday, January 28, 2021 10:29 AM

Examine Azure's AI services, and choose the right one for your company.

Overview

- Introduction 1 min
- Identify the product options 5 min
- Analyze the decision criteria 4 min
- Use Machine Learning for decision support systems 3 min
- Use Cognitive Services for data analysis 3 min
- Use Bot Service for interactive chat experiences 3 min
- Knowledge check 3 min
- Summary 1 min

From <https://docs.microsoft.com/en-us/learn/paths/az-900-describe-core-solutions-management-tools-azure/>

Introduction

- 1 minute

Artificial Intelligence (AI) is a category of computing that adapts and improves its decision-making ability over time based on its successes and failures. Microsoft Azure provides several AI solutions to choose from, each one depending on the problem you're trying to solve.

Tailwind Traders, a traditional brick-and-mortar retailer that has experienced explosive online sales growth, faces exciting challenges as it seeks to improve its e-commerce and service operations. Microsoft's AI services might be a good fit for one of the company's new initiatives, but Tailwind Traders needs help to better understand which product option is best for each scenario.

In this module, you'll learn about the various Microsoft AI services, and you'll analyze the decision criteria that experts use to select the right service for a specified scenario.

Learning objectives

After completing this module, you'll be able to:

- Choose the Azure AI services that best address your company's business challenges.

Prerequisites

- Familiarity with the concept of *application programming interfaces*, or APIs. Programmers use APIs to interact with the functionality that's contained in code libraries.

- Familiarity with the following additional concepts:
- *Web API*: An API that's accessible from servers that accept requests via HTTP.
- *Web API endpoint*: The location of the code library.
- *REST API*: The design of the URL style that's used to expose the API's functionality.

From <https://docs.microsoft.com/en-us/learn/modules/ai-machine-learning-fundamentals/1-introduction>

Identify the product options

- 5 minutes

AI is a broad classification of computing that allows a software system to perceive its environment and take action that maximizes its chance of successfully achieving its goals. A goal of AI is to create a software system that's able to adapt, or learn something on its own without being explicitly programmed to do it.

There are two basic approaches to AI. The first is to employ a *deep learning* system that's modeled on the neural network of the human mind, enabling it to discover, learn, and grow through experience.

The second approach is *machine learning*, a data science technique that uses existing data to train a model, test it, and then apply the model to new data to forecast future behaviors, outcomes, and trends.

Forecasts or predictions from machine learning can make apps and devices smarter. For example, when you shop online, machine learning powers product recommendation systems that offer additional products based on what you've bought and what other shoppers have bought who have purchased similar items in the past.

Machine learning is also used to detect credit card fraud by analyzing each new transaction and using what it has learned from analyzing millions of fraudulent transactions.

Virtually every device or software system that collects textual, visual, and audio data could feed a machine learning model that makes that device or software system smarter about how it functions in the future.

Azure product options

At a high level, there are three primary product offerings from Microsoft, each of which is designed for a specific audience and use case. Each option provides a diverse set of tools, services, and programmatic APIs. In this module, we'll merely scratch the surface of the options' capabilities.

Azure Machine Learning

Azure Machine Learning is a platform for making predictions. It consists of tools and services that allow you to connect to data to train and test models to find one that will most accurately predict a future result. After you've run experiments to test the model,

you can deploy and use it in real time via a web API endpoint.
With Azure Machine Learning, you can:

- Create a process that defines how to obtain data, how to handle missing or bad data, how to split the data into either a training set or test set, and deliver the data to the training process.
- Train and evaluate predictive models by using tools and programming languages familiar to data scientists.
- Create pipelines that define where and when to run the compute-intensive experiments that are required to score the algorithms based on the training and test data.
- Deploy the best-performing algorithm as an API to an endpoint so it can be consumed in real time by other applications.

Choose Azure Machine Learning when your data scientists need complete control over the design and training of an algorithm using your own data.

Azure Cognitive Services

Azure Cognitive Services provides prebuilt machine learning models that enable applications to see, hear, speak, understand, and even begin to reason. Use Azure Cognitive Services to solve general problems, such as analyzing text for emotional sentiment or analyzing images to recognize objects or faces. You don't need special machine learning or data science knowledge to use these services. Developers access Azure Cognitive Services via APIs and can easily include these features in just a few lines of code.
While Azure Machine Learning requires you to bring your own data and train models over that data, Azure Cognitive Services, for the most part, provides pretrained models so that you can bring in your live data to get predictions on.
Azure Cognitive Services can be divided into the following categories:

- Language services: Allow your apps to process natural language with prebuilt scripts, evaluate sentiment, and learn how to recognize what users want.
- Speech services: Convert speech into text and text into natural-sounding speech. Translate from one language to another and enable speaker verification and recognition.
- Vision services: Add recognition and identification capabilities when you're analyzing pictures, videos, and other visual content.
- Decision services: Add personalized recommendations for each user that automatically improve each time they're used, moderate content to monitor and remove offensive or risky content, and detect abnormalities in your time series data.

Azure Bot Service

Azure Bot Service and Bot Framework are platforms for creating virtual agents that

understand and reply to questions just like a human. Azure Bot Service is a bit different from Azure Machine Learning and Azure Cognitive Services in that it has a specific use case. Namely, it creates a virtual agent that can intelligently communicate with humans. Behind the scenes, the bot you build uses other Azure services, such as Azure Cognitive Services, to understand what their human counterparts are asking for.

Bots can be used to shift simple, repetitive tasks, such as taking a dinner reservation or gathering profile information, on to automated systems that might no longer require direct human intervention. Users converse with a bot by using text, interactive cards, and speech. A bot interaction can be a quick question and answer, or it can be a sophisticated conversation that intelligently provides access to services.

From <https://docs.microsoft.com/en-us/learn/modules/ai-machine-learning-fundamentals/2-identify-product-options>

Analyze the decision criteria

- 4 minutes

In this unit, you'll analyze the criteria that experts employ when they choose an AI service for a specific business need. Understanding the criteria can also help you better understand the nuanced differences among the products.

Are you building a virtual agent that interfaces with humans via natural language?

Use Azure Bot Service when you need to create a virtual agent to interact with humans by using natural language. Bot Service integrates knowledge sources, natural language processing, and form factors to allow interaction across different channels.

Bot Service solutions usually rely on other AI services for such things as natural language understanding or even translation for localizing replies into a customer's preferred language.

Before you jump in to build a custom chat experience by using Bot Service, it might make sense to search for prebuilt, no-code solutions that cover common scenarios. For example, you can use QnA Maker, which is available from Azure Marketplace, to build, train, and publish a sophisticated bot that uses FAQ pages, support websites, product manuals, SharePoint documents, or editorial content through an easy-to-use UI or via REST APIs.

Likewise, Power Virtual Agents integrates with Microsoft Power Platform so that you can use hundreds of prebuilt connectors for data input. You can extend Power Virtual Agents by building custom workflows with Power Automate, and if you feel that the out-of-the-box experience is too limiting, you can still build more complex interactions with Microsoft Bot Framework.

Do you need a service that can understand the content

and meaning of images, video, or audio, or that can translate text into a different language?

Use Azure Cognitive Services when it comes to general purpose tasks, such as performing speech to text, integrating with search, or identifying the objects in an image. Azure Cognitive Services is *general purpose*, meaning that many different kinds of customers can benefit from the work that Microsoft has already done to train and test these models and offer them inexpensively at scale.

Do you need to predict user behavior or provide users with personalized recommendations in your app?

The Azure Cognitive Services Personalizer service watches your users' actions within an application. You can use Personalizer to predict their behavior and provide relevant experiences as it identifies usage patterns. Here again, you could capture and store user behavior and create your own custom Azure Machine Learning solution to do these things, but this approach would require much effort and expense.

Will your app predict future outcomes based on private historical data?

Choose Azure Machine Learning when you need to analyze data to predict future outcomes. For example, suppose you need to analyze years' worth of financial transactions to discover new patterns that could help you create new products and services for your company's clients and then offer those new services during routine customer service calls. When you're working with proprietary data, you'll likely need to build a more custom-tailored machine learning model.

Do you need to build a model by using your own data or perform a different task than those listed above?

Use Azure Machine Learning for maximum flexibility. Data scientists and AI engineers can use the tools they're familiar with and the data you provide to develop deep learning and machine learning models that are tuned for your particular requirements.

From <https://docs.microsoft.com/en-us/learn/modules/ai-machine-learning-fundamentals/3-analyze-decision-criteria>

Use Machine Learning for decision support systems

- 3 minutes

The Tailwind Traders e-commerce website allows its customers to browse and purchase items that can be delivered or picked up from a retail store nearest to their location.
The Marketing team is convinced that it can increase sales dramatically by suggesting add-on products that complement the items in a shopper's cart at the point of checkout. The team could hard-code these suggestions, but it feels that a more organic approach would be to use its years' worth of sales data as well as new shopping trends to decide what products to display to the shopper. Additionally, the suggestions could be influenced by product availability, product profitability, and other factors.
The Marketing team's existing data science experts have already done some initial analysis of the problem domain, and have determined that its plan might take months to prototype, and possibly a year to roll out.

Which service should you choose?

Let's apply the decision criteria you learned about in the preceding unit to find the right option.
First, is Tailwind Traders building a virtual agent that interfaces with humans via natural language? No, it is not, so Azure Bot Service is not a good candidate for this scenario.
Second, does Tailwind Traders need a service that can understand the content and meaning of images, video, audio, or translate text into a different language? No, it doesn't, so the relevant Cognitive Services will not help the company.
Third, does Tailwind Traders need to predict user behavior or provide users with personalized recommendations? Yes, it does. However, creating recommendations based on user behavior is only part of the requirement. Tailwind Traders needs to create a complex model that incorporates historical sales data, trending sales data, inventory, and more. It's possible that the Azure Cognitive Services Personalizer service could play a role, but it couldn't handle the entire breadth of the project alone.
Fourth, will the Tailwind Traders app predict future outcomes based on private historical data? Yes, and that is why in this scenario, Azure Machine Learning is likely the best choice.
The success of this effort would depend primarily on the ability of the model to select precisely the right up-sale products to suggest to the shopper. Because the model would need to be tweaked and tuned over time, an off-the-shelf model would likely not suffice.
Finally, it sounds like the Marketing team already employs some data science experts, and the team is willing to make at least a year-long commitment to building, testing, and tweaking the models to be used.

From <https://docs.microsoft.com/en-us/learn/modules/ai-machine-learning-fundamentals/4-use-machine-learning>

Use Cognitive Services for data analysis

- 3 minutes

The first generation of the Tailwind Traders e-commerce website was available

exclusively in English. However, when the Marketing team sponsored a demographics study for the company's brick-and-mortar locations, it found that, on average, only 80 percent of potential customers speak English. In some neighborhoods, that number falls to 50 percent. The team sees the addition of multiple languages as a wonderful opportunity to serve non-English speakers with the same online e-commerce experience as English speakers.

Which service should you choose?

As in the preceding unit, apply the decision criteria you learned about earlier to find the right option.

First, is Tailwind Traders building a virtual agent that interfaces with humans via natural language? No, it is not, so Azure Bot Service is not a good candidate for this scenario. However, should Tailwind Traders ever implement a customer service agent, it might want to consider using the Translator API to provide real-time translation to help customers who are not English speakers.

Second, does Tailwind Traders need a service that can understand the content and meaning of images, video, audio, or translate text into a different language? Yes, it does. Translating textual content from one language into another is a general purpose task that you can simplify by using the Azure Cognitive Services Translator service. The service is easy to integrate into your applications, websites, tools, and solutions. It allows you to add multilanguage user experiences in more than 60 languages, and you can use it on any hardware platform with any operating system for text-to-text language translation.

Azure Cognitive Services is likely the best option for this scenario, but let's continue applying the decision criteria to make sure.

Third, does Tailwind Traders need to predict user behavior or provide users with personalized recommendations? No, it doesn't, so the Azure Cognitive Services Personalizer is not a good candidate for this scenario.

Finally, will the Tailwind Traders app need to predict future outcomes based on private historical data? No. Although it's possible to create a Machine Learning model for multilanguage translation, it would be expensive and time consuming for Tailwind Traders to attempt to build translation models themselves. The team has neither the deep learning competency nor the linguistic data that's required to train the models.

Now that you've examined all the expert criteria, you can confidently select Cognitive Services as the best product option for this scenario.

From <https://docs.microsoft.com/en-us/learn/modules/ai-machine-learning-fundamentals/5-use-cognitive-services>

Use Bot Service for interactive chat experiences

- 3 minutes

The Customer Service team has long asked for a virtual agent to handle the vast majority of questions it gets asked. No matter how prominent it makes the answers to

the most frequently asked questions on the website, shoppers are impatient and perceive contact in a chat window as saving them time.
The team wants shoppers to feel as though they're interacting with a real human. When it becomes clear that the virtual agent can't provide an answer, the chat session should be transferred to a human.
Providing a virtual agent would decrease the amount of time it takes for all shoppers to receive answers. The virtual agent could answer most questions, which would free up human customer service agents to provide support for more difficult questions or thorny account-related issues.

Which service should you choose?

Once again, apply the decision criteria you're now familiar with to find the right product. First, is Tailwind Traders building a virtual agent that interfaces with humans via natural language? Yes, it is. Azure Bot Service should be used in this scenario to implement a virtual agent chat experience. Bot Service could benefit from the information on the website's Frequently Asked Questions page, along with thousands of chat sessions that have been stored between shoppers and customer service representatives. Customer Service supervisors can test and tweak the answers to continue to refine the chat experience.
Even though you've likely found the best option for this scenario, keep applying the decision criteria to see whether any additional options might work.
Second, does Tailwind Traders need a service that can understand the content and meaning of images, video, audio, or translate text into a different language? Possibly, yes. In this scenario, Azure Cognitive Services could be used along with Bot Service to build the solution. To expedite implementation, the developers could explore using prebuilt solutions, such as QnA Maker (part of Cognitive Services) or Power Virtual Agents. Also, any Azure Bot solution would likely implement several Azure Cognitive Services, such as Language Understanding (LUIS) and possibly Translator, to translate from the shopper's language to English and back again.
Third, does Tailwind Traders need to predict user behavior or provide users with personalized recommendations? No, it doesn't. Azure Cognitive Services Personalizer is not a good candidate for this scenario.
Finally, will the Tailwind Traders app need to predict future outcomes based on private historical data? No. Although Tailwind Traders *does* have historical data to feed into a model, which would make it possible to use Azure Machine Learning to create a chat solution, another option is already tailored for the chat bot experience.

From <https://docs.microsoft.com/en-us/learn/modules/ai-machine-learning-fundamentals/6-use-bot-services>

Choose the best tools to help organizations build better solutions

Thursday, January 28, 2021 10:30 AM

Learn about Microsoft tools and services that help developers and operations engineers build modern solutions for the cloud and on-premises.

Overview

From <https://docs.microsoft.com/en-us/learn/paths/az-900-describe-core-solutions-management-tools-azure/>

Introduction

- 1 minute

Modern software development practices are supported by tools that encompass virtually every aspect of the software development life cycle. Microsoft has created a comprehensive set of tools that help organizations implement DevOps practices, develop solutions, and save money while doing so. In this module, you'll learn how to choose the right tools to support those practices.

Tailwind Traders has experimented with various software development processes and tools. Until now, however, there has been no organizational commitment to shift to a DevOps mindset. Likewise, there has been no planned, coordinated effort to standardize on a set of core tools and processes. Several new initiatives at the company accentuate the need for agile, repeatable, dependable management and deployment of software systems. Tailwind Traders believes that the adoption of DevOps tooling and practices is critical to the company's future success.

In this module, you'll learn about the various software development process tools that Microsoft offers. You'll explore the criteria that experts use to make their choices.

By the end of this module, you'll be able to choose the software development process tools and services that best align with your organization's goals and practices.

Learning objectives

After completing this module, you'll be able to:

- Choose the software development process tools and services that best address specific business scenarios.

Prerequisites

- A development or operations background is valuable but not required.
- Some familiarity with the concept of DevOps and its larger purpose in the organization, goals, outcomes, and so on.
- To help with understanding the value of the tools covered in this module, familiarity with such concepts as:
- Software development lifecycle
- Source-code management and version control
- The various forms of testing
- Continuous integration and continuous delivery, or CI/CD
- Continuous deployment
- Infrastructure as code

From <https://docs.microsoft.com/en-us/learn/modules/azure-devops-devtest-labs/1-introduction>

Understand your product options

- 4 minutes

Software developers and operations professionals strive to create working software systems that satisfy the needs of the organization. However, sometimes their short-term objectives are at cross-purposes, which can result in technical issues, delays, and downtime.

DevOps is a new approach that helps to align technical teams as they work toward common goals. To accomplish this alignment, organizations employ practices and processes that seek to automate the ongoing development, maintenance, and deployment of software systems. Their aim is to expedite the release of software changes, ensure the ongoing deployability of the system, and ensure that all changes meet a high quality bar.

When done correctly, DevOps practices and processes touch nearly every aspect of the company, not to mention the software development lifecycle, including planning, project management, and the collaboration of software developers with each other and with operations and quality assurance teams. Tooling automates and enforces most of the practices and processes, making it both difficult and unnecessary to work around.

DevOps requires a fundamental mindset change from the top down. Organizations can't merely install software tools or adopt services and hope to get all of the benefits promised by DevOps.

In this module, we'll focus only on the Microsoft tools that can help accomplish some of the DevOps objectives. Alternately, organizations that aren't ready to fully embrace the power of DevOps can support technical teams in their cloud development activities. If you're interested in learning more about DevOps in general, Microsoft Learn has several learning paths and modules that can help you.

Microsoft offers tools to enable source-code management, continuous integration and continuous delivery (CI/CD), and automating the creation of testing environments.

Sometimes, it seems as though these tools overlap in functionality, so in this module you'll learn about several product options, and when to choose one product over another.

Product options

At a high level, there are three primary offerings, each of which is aimed at a specific audience and use case and provides a diverse set of tools, services, programmatic APIs, and more.

Azure DevOps Services

Azure DevOps Services is a suite of services that address every stage of the software development lifecycle.

- Azure Repos is a centralized source-code repository where software development, DevOps engineering, and documentation professionals can publish their code for review and collaboration.
- Azure Boards is an agile project management suite that includes Kanban boards, reporting, and tracking ideas and work from high-level epics to work items and issues.
- Azure Pipelines is a CI/CD pipeline automation tool.
- Azure Artifacts is a repository for hosting artifacts, such as compiled source code, which can be fed into testing or deployment pipeline steps.
- Azure Test Plans is an automated test tool that can be used in a CI/CD pipeline to ensure quality before a software release.

Azure DevOps is a mature tool with a large feature set that began as on-premises server software and evolved into a software as a service (SaaS) offering from Microsoft.

GitHub and GitHub Actions

GitHub is arguably the world's most popular code repository for open-source software. Git is a decentralized source-code management tool, and GitHub is a hosted version of Git that serves as the primary remote. GitHub builds on top of Git to provide related services for coordinating work, reporting and discussing issues, providing documentation, and more. It offers the following functionality:

- It's a shared source-code repository, including tools that enable developers to perform code reviews by adding comments and questions in a web view of the source code before it can be merged into the main code base.
- It facilitates project management, including Kanban boards.
- It supports issue reporting, discussion, and tracking.
- It features CI/CD pipeline automation tooling.
- It includes a wiki for collaborative documentation.
- It can be run from the cloud or on-premises

Most relevant for this module, GitHub Actions enables workflow automation with triggers for many lifecycle events. One such example would be automating a CI/CD *toolchain*.

A toolchain is a combination of software tools that aid in the delivery, development, and management of software applications throughout a system's development lifecycle. The output of one tool in the toolchain is the input of the next tool in the toolchain. Typical tool functions range from performing automated dependency updates to building and configuring the software, delivering the build artifacts to various locations, testing, and so on.

With such similarity between many GitHub and Azure DevOps features, you might wonder which product to choose for your organization. Unfortunately, the answer might not be straightforward.

Although both Azure DevOps and GitHub allow public and private code repositories, GitHub has a long history with public repositories and is trusted by tens of thousands of open-source project owners. GitHub is a lighter-weight tool than Azure DevOps, with a focus on individual developers contributing to the open-source code. Azure DevOps, on the other hand, is more focused on enterprise development, with heavier project-management and planning tools, and finer-grained access control.

Note

Your choices are not limited to Azure DevOps Services or GitHub and GitHub Actions. In practice, you can mix and match these services as needed. For example, you can use GitHub repos with Azure Boards for work item tracking.

Azure DevTest Labs

Azure DevTest Labs provides an automated means of managing the process of building, setting up, and tearing down virtual machines (VMs) that contain builds of your software projects. This way, developers and testers can perform tests across a variety of environments and builds. And this capability isn't limited to VMs. Anything you can deploy in Azure via an ARM template can be provisioned through DevTest Labs.

Provisioning pre-created lab environments with their required configurations and tools already installed is a huge time saver for quality assurance professionals and developers. Suppose you need to test a new feature on an old version of an operating system. Azure DevTest Labs can set up everything automatically upon request. After the testing is complete, DevTest Labs can shut down and deprovision the VM, which saves money when it's not in use. To control costs, the management team can restrict how many labs can be created, how long they run, and so on.

From <https://docs.microsoft.com/en-us/learn/modules/azure-devops-devtest-labs/2-identify-product-options>

Analyze the decision criteria

- 4 minutes

In this unit, you'll analyze the criteria that experts employ when they choose DevOps

tools or services to address specific business needs. Understanding the criteria can also help you better understand the nuanced differences between each product.

Do you need to automate and manage test-lab creation?

If your aim is to automate the creation and management of a test lab environment, consider choosing Azure DevTest Labs. Among the three tools and services we've described, it's the only one that offers this functionality.
However, you can automate the provisioning of new labs as part of a toolchain by using Azure Pipelines or GitHub Actions.

Are you building open-source software?

Although Azure DevOps can publish public code repositories, GitHub has long been the preferred host for open-source software. If you're building open-source software, you would likely choose GitHub if for no other reasons than its visibility and general acceptance by the open-source development community.
The remaining decision criteria are specific to choosing between either Azure DevOps or GitHub.

Note

Your choices aren't limited to Azure DevOps Services or GitHub and GitHub Actions. In practice, you can mix and match these services as needed. For example, you can use GitHub repos with Azure Boards for work-item tracking.

Regarding source-code management and DevOps tools, what level of granularity do you need for permissions?

GitHub works on a simple model of read/write permissions to every feature. Meanwhile, Azure DevOps has a much more granular set of permissions that allow organizations to refine who is able to perform most operations across the entire toolset.

Regarding source-code management and DevOps tools, how sophisticated does your project management and reporting need to be?

Although GitHub has work items, issues, and a Kanban board, project management and reporting is the area where Azure DevOps excels. Azure DevOps is highly customizable, which allows an administrator to add custom fields to capture metadata and other information alongside each work item. By contrast, the GitHub Issues feature uses tags as its primary means of helping a team categorize issues.

Regarding source-code management and DevOps tools, how tightly do you need to integrate with third-party tools?

Although we make no specific recommendations about third-party tools, it's important

for you to understand your organization's existing investments in tools and services and to evaluate how these dependencies might affect your choice. It's likely that most vendors that create DevOps tools create hooks or APIs that can be used by both Azure Pipelines and GitHub Actions. Even so, it's probably worth the effort to validate that assumption.

From <https://docs.microsoft.com/en-us/learn/modules/azure-devops-devtest-labs/3-analyze-decision-criteria>

Use Azure DevOps to manage the application development lifecycle

- 3 minutes

The software development team at Tailwind Traders works on many different projects, both for internal and external usage. The team needs to give project sponsors and managers executive level reporting, including burndown charts, track progress against epics, and track custom information that's specific to Tailwind Traders in each work item and bug report.

As Tailwind Traders grows and hires contractors and outside vendors for short-term work, the upper management team wants to ensure that these individuals have access only to the information they need to do their work.

Which services should we choose?

Apply the decision criteria you learned about in the preceding unit to find the right option.

First, does Tailwind Traders need to automate and manage test lab creation? No. So, in this scenario, Azure DevTest Labs is not a candidate, because it isn't intended for this specific use case.

Second, is Tailwind Traders building open-source software? Though it's not stated specifically, Tailwind Traders is building internal and external systems, such as their e-commerce system, which isn't open source. So that isn't a consideration in this scenario.

Third, what level of granularity does Tailwind Traders need for permissions? Earlier, we stated that Tailwind Traders will hire temporary employees and vendors for short-term work, which makes a granular permissions requirement an important consideration for upper management. Based on our description in the preceding unit, this feature would make Azure DevOps a leading candidate. By using Azure DevOps, Tailwind Traders administrators would also have a more robust set of options for controlling permissions across the entire portfolio of work.

Fourth, does Tailwind Traders require a sophisticated project management and reporting solution? Yes, robust project management and reporting features are one of the primary considerations. Here again, because of the amount of work-item customization and reporting the management team wants, Azure DevOps would likely be a good choice.

Fifth, does Tailwind Traders require tight integration with any third-party DevOps tools? Tool integration was not listed as a primary consideration for this scenario. As you learned in the preceding unit, most third-party DevOps tools integrate with both Azure DevOps and GitHub, which makes it likely that the team will find the tools it needs.

From <https://docs.microsoft.com/en-us/learn/modules/azure-devops-devtest-labs/4-use-azure-devops>

Use GitHub to contribute to open-source software

- 3 minutes

Tailwind Traders hopes to publish an API that would allow third parties to integrate their own inventories of new and used items. This approach would allow Tailwind Traders to offer a wider variety of products directly from their e-commerce site.

Although the internal implementation of the API is closed source, Tailwind Traders wants to create a set of examples that call the API to perform various actions. The team needs a platform to share example code, collect feedback on the API, allow contributors to report issues, and build a community around feature requests.

Which service should you choose?

Apply the decision criteria you learned about earlier to find the right option.

First, does Tailwind Traders need to automate and manage test lab creation? No. In this scenario, Azure DevTest Labs is not a candidate because it isn't designed for this use case.

Second, is Tailwind Traders building open-source software? Yes. As we noted in a previous unit, developers are used to seeing this kind of content available on GitHub. With GitHub, Tailwind Traders developers can publish their code, accept community contributions to improve the code examples, accept feedback and bug reports, and more. Because this scenario involves open-source code, GitHub is a leading candidate.

Third, what level of granularity does the Tailwind Traders team need for assigning permissions? Though it's not stated explicitly, the fact that Tailwind Traders will be accepting community contributions, issuing reports, and generally attempting to build a community of developers around their API examples, the company's permission needs are basic: users can either *view only* or *view and write*. This is another reason why GitHub would be a good candidate for this scenario.

Fourth, does Tailwind Traders require a sophisticated project management and reporting solution? Again, because of the nature of this project, the team doesn't require a sophisticated project management and reporting solution. In this scenario, the strength of Azure DevOps Services isn't required.

Fifth, does Tailwind Traders require tight integration with any third-party DevOps tools? Tool integration wasn't listed as a primary consideration for this scenario and doesn't qualify or disqualify either tool.

GitHub is the best choice for this scenario. Although you could use Azure DevOps to make the repository public, some of the other features that involve the development community, such as feedback or bug reports, would be less accessible.

From <https://docs.microsoft.com/en-us/learn/modules/azure-devops-devtest-labs/5-use-github>

Use Azure DevTest Labs to manage testing environments

- 2 minutes

Tailwind Traders wants to be more methodical and careful when it pushes new versions of its e-commerce website to production. The company will expand its quality assurance (QA) team, and it will use the cloud to create and host virtual machines (VMs). Through this approach, it will create testing environments that match the production environment.

The management team has concerns around the costs of a more automated test environment. For instance, it wants to make sure that the QA professionals are not wasting time configuring the testing environment to match the production environment. The team wants to ensure that the VMs are destroyed when they're no longer in use. It wants to limit the number of VMs that each QA professional is allowed to spin up. Also, the team wants to ensure that each environment is configured correctly and consistent with the production environment.

Which service should you choose?

Once again, start by applying the decision criteria you learned about previously to find the right product.

First, does Tailwind Traders need to automate and manage test lab creation? Yes. This looks like a job for Azure DevTest Labs, because it can do everything that the team needs to accomplish in this scenario.

We could continue evaluating the decision criteria, but neither Azure DevOps nor GitHub is needed for this scenario. Remember that either Azure DevOps or GitHub could be used to create product releases that can automatically be included in any VMs that you create for testing purposes.

From <https://docs.microsoft.com/en-us/learn/modules/azure-devops-devtest-labs/6-use-azure-devtest-labs>

Choose the best monitoring service for visibility, insight, and outage mitigation

Thursday, January 28, 2021 10:32 AM

Learn about solutions that can give your IT organization insight into the health and performance of its cloud-based applications.

Overview

- Introduction 2 min
- Identify your product options 4 min
- Analyze the decision criteria 3 min
- Use Azure Advisor 3 min
- Use Azure Monitor 3 min
- Use Azure Service Health 3 min
- Knowledge check 3 min
- Summary 1 min

From <https://docs.microsoft.com/en-us/learn/paths/az-900-describe-core-solutions-management-tools-azure/>

Introduction

- 2 minutes

Modern software systems running in the cloud are complex, and gaining visibility into the health and performance of your application-hosting environment across all of its layers of services is challenging. Fortunately, there are several solutions from Microsoft that can help you react quickly to outages, research intermittent issues, optimize your usage, and be proactive in handling future planned downtime.

Tailwind Traders, a traditional brick-and-mortar retailer, is now experiencing explosive growth by selling products online. The company is seeking to tighten and operationalize control of its cloud environment. It faces several challenges, from needing to optimize its cloud spend and security posture to tracking intermittent issues and planning ahead for upcoming outages. However, the company needs help with choosing the right product option for each of these scenarios.

In this module, you'll learn about the several Microsoft monitoring solutions, and you'll analyze decision criteria that experts use to select the right service for a specific scenario.

Learning objectives

After completing this module, you'll be able to:

- Choose the cloud monitoring service that best addresses your company's business challenges.

Prerequisites

- Familiarity with basic computing concepts and terminology
- Familiarity with cloud computing is helpful but not necessary

From <https://docs.microsoft.com/en-us/learn/modules/monitoring-fundamentals/1-introduction>

Identify your product options

- 4 minutes

Several basic questions or concerns face all companies that use the cloud.

- Are we using the cloud correctly? Can we squeeze more performance out of our cloud spend?
- Are we spending more than we need to?
- Do we have our systems properly secured?
- How resilient are our resources? If we experience a regional outage, could we fail over to another region?
- How can we diagnose and fix issues that occur intermittently?
- How can we quickly determine the cause of an outage?
- How can we learn about planned downtime?

Fortunately, by using a combination of monitoring solutions on Azure, you can:

- Gain answers, insights, and alerts to help ensure that you've optimized your cloud usage.
- Ascertain the root cause of unplanned issues.
- Prepare ahead of time for planned outages.

The product options

At a high level, there are three primary Azure monitoring offerings, each of which is aimed at a specific audience and use case and provides a diverse set of tools, services, programmatic APIs, and more.

Azure Advisor

Azure Advisor evaluates your Azure resources and makes recommendations to help improve reliability, security, and performance, achieve operational excellence, and reduce costs. Advisor is designed to help you save time on cloud optimization. The recommendation service includes suggested actions you can take right away, postpone, or dismiss.

The recommendations are available via the Azure portal and the API, and you can set up notifications to alert you to new recommendations.

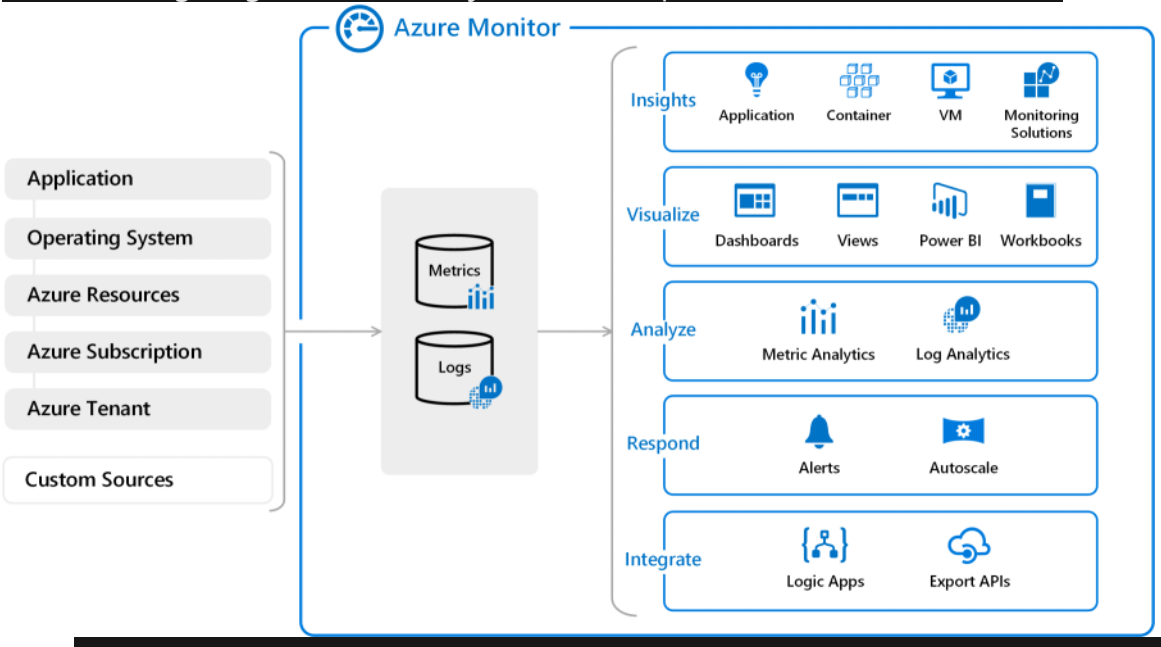
When you're in the Azure portal, the Advisor dashboard displays personalized recommendations for all your subscriptions, and you can use filters to select recommendations for specific subscriptions, resource groups, or services. The recommendations are divided into five categories:

- Reliability: Used to ensure and improve the continuity of your business-critical

applications.
- Security: Used to detect threats and vulnerabilities that might lead to security breaches.
- Performance: Used to improve the speed of your applications.
- Cost: Used to optimize and reduce your overall Azure spending.
- Operational Excellence: Used to help you achieve process and workflow efficiency, resource manageability, and deployment best practices.

Azure Monitor

Azure Monitor is a platform for collecting, analyzing, visualizing, and potentially taking action based on the metric and logging data from your entire Azure and on-premises environment.
The following diagram illustrates just how comprehensive Azure Monitor is.



- On the left is a list of the sources of logging and metric data that can be collected at every layer in your application architecture, from application to operating system and network.
- In the center, you can see how the logging and metric data is stored in central repositories.
- On the right, the data is used in a number of ways. You can view real-time and historical performance across each layer of your architecture, or aggregated and detailed information. The data is displayed at different levels for different audiences. You can view high-level reports on the Azure Monitor Dashboard or create custom views by using Power BI and Kusto queries.

Additionally, you can use the data to help you react to critical events in real time, through alerts delivered to teams via SMS, email, and so on. Or you can use thresholds to trigger autoscaling functionality to scale up or down to meet the demand.
Some popular products such as Azure Application Insights, a service for sending telemetry information from application source code to Azure, uses Azure Monitor under

the hood. With Application Insights, your application developers can take advantage of the powerful data-analysis platform in Azure Monitor to gain deep insights into an application's operations and diagnose errors without having to wait for users to report them.

Azure Service Health

Azure Service Health provides a personalized view of the health of the Azure services, regions, and resources you rely on. The status.azure.com website, which displays only major issues that broadly affect Azure customers, doesn't provide the full picture. But Azure Service Health displays both major and smaller, localized issues that affect you. Service issues are rare, but it's important to be prepared for the unexpected. You can set up alerts that help you triage outages and planned maintenance. After an outage, Service Health provides official incident reports, called root cause analyses (RCAs), which you can share with stakeholders.
Service Health helps you keep an eye on several event types:

- Service issues are problems in Azure, such as outages, that affect you right now. You can drill down to the affected services, regions, updates from your engineering teams, and find ways to share and track the latest information.
- Planned maintenance events can affect your availability. You can drill down to the affected services, regions, and details to show how an event will affect you and what you need to do. Most of these events occur without any impact to you and aren't shown here. In the rare case that a reboot is required, Service Health allows you to choose when to perform the maintenance to minimize the downtime.
- Health advisories are issues that require you to act to avoid service interruption, including service retirements and breaking changes. Health advisories are announced far in advance to allow you to plan.

From <https://docs.microsoft.com/en-us/learn/modules/monitoring-fundamentals/2-identify-product-options>

Analyze the decision criteria

- 3 minutes

In this unit, you'll analyze the criteria that experts employ when they choose an Azure monitoring service for a specified business need. By understanding the criteria, you can better assess the nuanced differences among the products.

Do you need to analyze how you're using Azure to reduce costs? Improve resilience? Harden your security?

Choose Azure Advisor when you're looking for an analysis of your deployed resources. Azure Advisor analyzes the configuration and usage of your resources and provides suggestions on how to optimize for reliability, security, performance, costs, and

operations based on experts' best practices.

Do you want to monitor Azure services or your usage of Azure?

If you want to keep tabs on Azure itself, especially the services and regions you depend on, you want to choose Azure Service Health. You can view the current status of the Azure services you rely on, upcoming planned outages, and services that will be sunset. You can set up alerts that help you stay on top of incidents and upcoming downtime without having to visit the dashboard regularly.
However, if you want to keep track of the performance or issues related to your specific VM or container instances, databases, your applications, and so on, you want to visit Azure Monitor and create reports and notifications to help you understand how your services are performing or diagnose issues related to your Azure usage.

Do you want to measure custom events alongside other usage metrics?

Choose Azure Monitor when you want to measure custom events alongside other collected telemetry data. Custom events, such as those added in the source code of your software applications, could help identify and diagnose why your application is behaving a certain way.

Do you need to set up alerts for outages or when autoscaling is about to deploy new instances?

Here again, you would use Azure Monitor to set up alerts for key events that are related to your specific resources.

From <https://docs.microsoft.com/en-us/learn/modules/monitoring-fundamentals/3-analyze-decision-criteria>

Use Azure Advisor

- 3 minutes

Tailwind Traders wants to optimize its cloud spend. Also, the organization is concerned about security breaches, because it stores customer data and historical purchase data in cloud-based databases. As the organization ramps up its cloud expertise, it wants to better understand its use of the cloud, better understand best practices, and pinpoint "easy wins" where it can tighten up its cloud spend and security practices.

Which service should you choose?

Apply the decision criteria you learned about in the preceding unit to find the right

option.
First, in this scenario, does Tailwind Traders need to analyze its Azure usage for the sake of optimization? Yes. Tailwind Traders understands that it might be spending too much, is concerned about its security practices, and wants to have its cloud usage analyzed against industry best practices. Therefore, Azure Advisor is the perfect option for this scenario.
Although you might have found the right product option, let's continue evaluating the decision criteria for this scenario.
Second, in this scenario, does Tailwind Traders want to monitor the health of Azure services that affect all customers or the resources that are deployed on Azure? This scenario isn't concerned with operations. However, Azure Advisor does analyze and provide recommendations for achieving operational excellence.
Third, in this scenario, does Tailwind Traders want to measure custom events alongside other usage metrics? No, measuring custom events isn't mentioned as a requirement and isn't a consideration in this scenario.
Fourth, in this scenario, does Tailwind Traders want to set up alerts for outages or when autoscaling is about to deploy new instances? Again, this scenario isn't concerned with operations. However, Azure Advisor does analyze and provide recommendations for achieving operational excellence.
Azure Advisor is the right product option to help Tailwind Traders better understand and optimize both its cloud spend and its cloud security posture. This product might help the organization with other areas of its cloud usage as well.

From <https://docs.microsoft.com/en-us/learn/modules/monitoring-fundamentals/4-use-azure-advisor>

Use Azure Monitor

- 3 minutes

The Tailwind Traders e-commerce website is experiencing intermittent errors, and the team is unsure of the cause. Because of the nature of the errors, the team suspects that it's either a database or caching issue. What are the circumstances surrounding the errors? Does it happen only during peak usage times? What is the state of the team's Azure SQL instance? What is the state of its Redis caching server? How can it trace the issues to a root cause?

Which service should you choose?

As in the preceding unit, apply the decision criteria that you learned about earlier to find the right option.
First, in this scenario, does Tailwind Traders need an analysis of its Azure usage for the sake of optimization? No, optimization isn't the team's objective in this scenario, so Azure Advisor isn't a candidate.
Second, in this scenario, does Tailwind Traders want to monitor the health of Azure services that affect all customers or the resources deployed on Azure? Because this issue

happens intermittently, it's unlikely to affect an entire Azure region or service. It's more likely that a logic issue exists somewhere in their e-commerce website code, or another issue is causing database failures or caching locks. In this scenario, the team could use Azure Monitor to pinpoint a specific user session and look at the performance of each service that's involved in the issue.
Third, in this scenario, does Tailwind Traders want to measure custom events alongside other usage metrics? Yes. Software developers can send additional information about the state of the web application via Application Insights to help locate the root cause of the issue. Application Insights relies on the Azure Monitor platform to store custom event information.
Fourth, in this scenario, does Tailwind Traders want to set up alerts for outages or for when autoscaling is about to deploy new instances? No, alerting isn't their objective in this scenario.
Azure Monitor is the best option for helping Tailwind Traders track this intermittent issue. The team can use a wealth of tools to help it gain insight into the application's performance at a high level and dive deep into specific issues.

From <https://docs.microsoft.com/en-us/learn/modules/monitoring-fundamentals/5-use-azure-monitor>

Use Azure Service Health

- 3 minutes

Tailwind Traders wants to operationalize its cloud environment. Specifically, its cloud operations team wants to let stakeholders know about upcoming planned downtime in advance. The team also wants its solution architects to be forewarned about any Microsoft plans to sunset services so it can rearchitect its software products accordingly. When outages do happen, the team wants to quickly ascertain whether the issue is specific to their services or a service interruption that affects many Azure customers. The team also wants to provide key stakeholders with reports that explain how and why the incident occurred, and so on.

Which service should you choose?

Again, apply the decision criteria you learned about earlier to find the right product.
First, in this scenario, does Tailwind Traders need to analyze its Azure usage for the sake of optimization? No, so Azure Advisor isn't a candidate for this scenario.
Second, does Tailwind Traders want to monitor the health of Azure services that affect all customers or the resources deployed on Azure? In this scenario, the requirement is to stay abreast of upcoming planned downtime. Additionally, the team wants to capture official incident reports. For this reason, Azure Service Health is the strongest candidate to choose for this scenario.
Although it's likely that you would choose Azure Service Health, let's continue evaluating the remaining decision criteria.
Third, in this scenario, does Tailwind Traders want to measure custom events alongside

other usage metrics? No, measuring custom events isn't mentioned as a requirement and isn't a consideration in this scenario.
Fourth, in this scenario, does Tailwind Traders want to set up alerts for outages or when autoscaling is about to deploy new instances? Setting up alerts for outages is a requirement in this scenario, but creating alerts for other events such as autoscaling are not in scope. Use Azure Service Health to set up alerts that are specific to Azure outages that affect all Azure customers. Use Azure Monitor to set up alerts for outages and other events that affect only your specific resources.
In this scenario, Azure Service Health is the correct option to choose.

From <https://docs.microsoft.com/en-us/learn/modules/monitoring-fundamentals/6-use-azure-service-health>

Choose the best tools for managing and configuring your Azure environment

Thursday, January 28, 2021 10:37 AM

Explore the Azure management, administration, and reporting tools, and choose the ones that best meet your organization's needs.

Overview

From <https://docs.microsoft.com/en-us/learn/paths/az-900-describe-core-solutions-management-tools-azure/>

Introduction

- 1 minute

By using Azure management tools, administrators, developers, and managers can interact with the cloud environment to perform such tasks as:

- Deploying dozens or hundreds of resources at a time.
- Configuring individual services programmatically.
- Viewing rich reports across usage, health, costs, and more.

Microsoft Azure provides a collection of management tooling options to choose from, depending on the situation.

Tailwind Traders, a traditional brick-and-mortar retailer, is now experiencing explosive growth by selling products online. The company owes much of its success to an ability to quickly and efficiently manage its cloud environment. As it began its cloud journey, Tailwind Traders initially had to choose the right management tools for its business needs.

In this module, you'll explore the array of Azure management tools and the decision criteria that experts use to select the right ones for their specific scenarios.

Learning objectives

After completing this module, you'll be able to:

- Choose the Azure management tools that best address your organization's

technical needs and challenges.

Prerequisites

- Familiarity with basic computing concepts and terminology
- Familiarity with cloud computing is helpful but not necessary

From <https://docs.microsoft.com/en-us/learn/modules/management-fundamentals/1-introduction>

Identify the product options

- 5 minutes

At a high level, there are two broad categories of management tools: visual tools and code-based tools.

Visual tools provide full, visually friendly access to all the functionality of Azure. However, visual tools might be less useful when you're trying to set up a large deployment of resources with interdependencies and configuration options.

When you're attempting to quickly set up and configure Azure resources, a code-based tool is usually the better choice. Although it might take time to understand the right commands and parameters at first, after they've been entered, they can be saved into files and used repeatedly as needed. Also, the code that performs setup and configuration can be stored, versioned, and maintained along with application source code in a source code-management tool such as Git. This approach to managing hardware and cloud resources, which developers use when they write application code, is referred to as *infrastructure as code*.

There are two approaches to infrastructure as code: *imperative* code and *declarative* code. Imperative code details each individual step that should be performed to achieve a desired outcome. By contrast, declarative code details only a desired outcome, and it allows an interpreter to decide how to best achieve that outcome. This distinction is important because tools that are based on declarative code can provide a more robust approach to deploying dozens or hundreds of resources simultaneously and reliably.

Your product options

Microsoft offers a variety of tools and services to manage your cloud environment, each aimed at different scenarios and users.

The Azure portal

By using the Azure portal, a web-based user interface, you can access virtually every feature of Azure. The Azure portal provides a friendly, graphical UI to view all the

services you're using, create new services, configure your services, and view reports. The Azure portal is how most users first experience Azure. But, as your Azure usage grows, you'll likely choose a more repeatable code-centric approach to managing your Azure resources.

The Azure mobile app

The Azure mobile app provides iOS and Android access to your Azure resources when you're away from your computer. With it, you can:

- Monitor the health and status of your Azure resources.
- Check for alerts, quickly diagnose and fix issues, and restart a web app or virtual machine (VM).
- Run the Azure CLI or Azure PowerShell commands to manage your Azure resources.

Azure PowerShell

Azure PowerShell is a shell with which developers and DevOps and IT professionals can execute commands called cmdlets (pronounced *command-lets*). These commands call the Azure Rest API to perform every possible management task in Azure. Cmdlets can be executed independently or combined into a script file and executed together to orchestrate:

- The routine setup, teardown, and maintenance of a single resource or multiple connected resources.
- The deployment of an entire infrastructure, which might contain dozens or hundreds of resources, from imperative code.

Capturing the commands in a script makes the process repeatable and automatable. Azure PowerShell is available for Windows, Linux, and Mac, and you can access it in a web browser via Azure Cloud Shell.

Windows PowerShell has helped Windows-centric IT organizations automate many of their on-premises operations for years, and these organizations have built up a large catalog of custom scripts and cmdlets, as well as expertise.

The Azure CLI

The Azure CLI command-line interface is an executable program with which a developer, DevOps professional, or IT professional can execute commands in Bash. The commands call the Azure Rest API to perform every possible management task in Azure. You can run the commands independently or combined into a script and executed together for the routine setup, teardown, and maintenance of a single resource or an entire environment.

In many respects, the Azure CLI is almost identical to Azure PowerShell in what you can do with it. Both run on Windows, Linux, and Mac, and can be accessed in a web browser

via Cloud Shell. The primary difference is the syntax you use. If you're already proficient in PowerShell or Bash, you can use the tool you prefer.

ARM templates

Although it's possible to write imperative code in Azure PowerShell or the Azure CLI to set up and tear down one Azure resource or orchestrate an infrastructure comprising hundreds of resources, there's a better way to implement this functionality.
By using Azure Resource Manager templates (ARM templates), you can describe the resources you want to use in a declarative JSON format. The benefit is that the entire ARM template is verified before any code is executed to ensure that the resources will be created and connected correctly. The template then orchestrates the creation of those resources in parallel. That is, if you need 50 instances of the same resource, all 50 instances are created at the same time.
Ultimately, the developer, DevOps professional, or IT professional needs only to define the desired state and configuration of each resource in the ARM template, and the template does the rest. Templates can even execute PowerShell and Bash scripts before or after the resource has been set up.

From <https://docs.microsoft.com/en-us/learn/modules/management-fundamentals/2-identify-product-options>

Analyze the decision criteria

- 3 minutes

In this unit, you'll analyze the criteria that experts employ to help them decide which Azure management tools to use to address their business needs. Understanding the criteria can help you to better understand the nuanced differences among the products.

Do you need to perform one-off management, administrative, or reporting actions?

Use either Azure PowerShell or the Azure CLI if you need to quickly obtain the IP address of a virtual machine (VM) you've deployed, reboot a VM, or scale an app. You might want to keep custom scripts handy on your local hard drive for certain operations that you perform occasionally.
By contrast, Azure Resource Manager templates (ARM templates) express the infrastructure requirements for your application for a repeatable deployment. ARM templates aren't intended for one-off scenarios but, depending on the scenario, it's possible to use them for this purpose. In these instances, you should prefer PowerShell, Azure CLI scripts, or the Azure portal.
Also, ARM templates can include PowerShell or Azure CLI scripts, which can trigger the execution of ARM templates. This gives you flexibility in choosing the right tool for your particular needs.

You could perform most, if not all, management and administrative actions via the Azure portal. If you're just learning Azure, need to set up and manage resources infrequently, or prefer a visual interface for viewing reports, it makes sense to take advantage of the visual presentation that the Azure portal offers.
However, if you're in a cloud management or administrative role, it's less efficient to rely solely on visual scanning and clicking. To find the settings and information you want to work with, it's often quicker and more repeatable to use the Azure CLI or PowerShell.
The last option in this case is the Azure mobile app, which you can access via an iOS or Android phone or tablet. Because it's full featured, it's likely the best choice when a laptop isn't readily available and you need to view and triage issues immediately.

Do you need a way to repeatedly set up one or more resources and ensure that all the dependencies are created in the proper order?

ARM templates express your application's infrastructure requirements for a repeatable deployment. A validation step ensures that all resources can be created, so that the resources are created in the proper order based on dependencies, in parallel, and idempotent.
By contrast, it's entirely possible to use either PowerShell or the Azure CLI to set up all the resources for a deployment. However, there's no validation step in these tools. If a script encounters an error, the dependency resources can't be rolled back easily, deployments happen serially, and only some operations are idempotent.

When you're scripting, do you come from a Windows administration or Linux administration background?

If you or your cloud administrators come from a Windows administration background, it's likely you'll prefer PowerShell. If you or your cloud administrators come from a Linux administration background, it's likely you'll prefer the Azure CLI. In practice, either tool can be used to perform most one-off administration tasks.

From <https://docs.microsoft.com/en-us/learn/modules/management-fundamentals/3-analyze-decision-criteria>

Use the Azure portal to visually understand and manage your cloud environment

- 3 minutes

Tailwind Traders uses Azure extensively throughout its entire organization. To make sure that both the technical and executive teams are aware of the company's cloud spend, the director of cloud operations will begin to meet weekly with the chief financial officer (CFO) to talk about their cloud spend.
Conversations might begin at a high level, but the two officers might want to dive deep

during the meeting to gain more insight into how Azure resources are being used. Ideally, they would be able to see the data displayed visually, but also be able to run custom reports in real time. Which tool can they use during their meeting?

Which service should you choose?

Apply the decision criteria you learned about in the preceding unit to find the right option.
First, in this scenario, does Tailwind Traders need to perform one-off management, administrative, or reporting actions? Yes, and given the requirement to view data visually and create custom reports during the meeting, the Azure portal is the best choice. The meeting attendees can quickly find answers to their questions by using a wealth of reporting options.
The next two decision criteria don't apply to this scenario, because the director of cloud operations and the CFO won't be deploying or configuring any resources.
The Azure portal is the correct product option for this scenario.

From <https://docs.microsoft.com/en-us/learn/modules/management-fundamentals/4-use-azure-portal>

Use Azure PowerShell for one-off administrative tasks

- 3 minutes

Tailwind Traders employs technologists with many different skills. A team of developers and administrators builds and maintains a collection of intranet applications that are vital to the business. The team members have strong backgrounds in Windows development and network administration.
The team moved its applications to the cloud, and it now needs a way to perform one-off testing, management, and administrative tasks in its intranet environment. The team quickly realized that managing Azure from the portal takes too much time and is not repeatable. Which tool should the company use for one-off tasks?

Which service should you choose?

As you did in the preceding unit, apply the decision criteria you learned about earlier to find the right option.
First, in this scenario, does the Tailwind Traders team need to perform one-off management, administrative, or reporting tasks? Yes. However, the team already knows that it doesn't want to rely on the Azure portal for these one-off actions. Therefore, both Azure PowerShell and the Azure CLI are good options. We'll hone in on which tool the team should use in a moment.
Second, in this scenario, does Tailwind Traders need a repeatable and reliable means of deploying its entire infrastructure? No, not in this scenario. Therefore, Azure Resource

Manager templates (ARM templates) are not the right choice.
When the Tailwind Traders team is doing scripting, does it come from a Windows administration or Linux administration background? This team has a Windows administration background. It would likely be most comfortable using Azure PowerShell, because this tool allows it to use the syntax it's most comfortable with to perform one-off administration tasks.
Azure PowerShell is the best choice for this scenario.

From <https://docs.microsoft.com/en-us/learn/modules/management-fundamentals/5-use-azure-powershell>

Use the Azure CLI for one-off administrative tasks

- 3 minutes

As we noted in the preceding unit, Tailwind Traders employs technologists with many different skills. The DevOps team is primarily concerned with keeping external systems, such as the company's e-commerce site, up and running. This team has a Linux administration background. It frequently needs to perform administrative tasks related to the health of the cloud environment. The team quickly realized that managing Azure from the portal takes too much time and isn't repeatable. Which tool should it use for one-off tasks?

Which service should you choose?

Once again, apply the decision criteria you learned about earlier to find the right option. Because this scenario is almost identical to the one in the preceding unit, you can skip over the first two criteria. In other words, you can quickly eliminate Azure Resource Manager templates (ARM templates) and the Azure portal as viable options for this scenario. So, let's go to the third decision criterion.
Choosing the right option in this scenario should be determined by the team's background. Because this team has a Linux administration background, it would likely be most comfortable using the Azure CLI. The Azure CLI allows the team to use the Bash shell and its syntax to perform one-off administration tasks.
The Azure CLI is the best choice for this scenario.

From <https://docs.microsoft.com/en-us/learn/modules/management-fundamentals/6-use-azure-cli>

Use the Azure mobile app to manage Azure on the go

- 2 minutes

Tailwind Traders experiences surges in e-commerce traffic that coincide with national holidays and weekends. In the company's first few years, managers of critical systems had to convene at the office of the director of cloud operations during these important periods. However, now that Tailwind Traders has successfully operationalized most critical systems, the director wants to relax this requirement and allow employees to

spend these dates with their families. Is there a product that can help support this scenario?

Which service should you choose?

Let's run through our decision criteria again.
First, does Tailwind Traders need to perform one-off management, administrative, reporting actions? Yes. The real question is, how? A phone or tablet solution could help key employees keep an eye on the health of the cloud environment when they're out of the office. The Azure mobile app is likely a good compromise, because it lets employees be away from work and still perform essential, one-off management and administrative tasks.
We can skip the rest of the decision criteria in this unique scenario. The Azure mobile app is the right choice.

From <https://docs.microsoft.com/en-us/learn/modules/management-fundamentals/7-use-azure-mobile-app>

Use ARM templates to deploy an entire cloud infrastructure

- 3 minutes

Tailwind Traders wants to operationalize their cloud deployments. The company needs a repeatable, reliable way to scale its operations during peak sales periods. Because you'll be choosing a process for scaling your production environment, you need to ensure that your chosen service:

- Is efficient and can potentially create many resources in parallel.
- Creates all dependencies in the correct order.
- Can be used without worrying that it failed in the middle of provisioning the necessary infrastructure.

Which service should you choose?

Let's run through the decision criteria one more time.
First, in this scenario, does Tailwind Traders need to perform one-off management, administrative, or reporting actions? This time, we're not looking to support one-time or one-off management or administration tasks. We're looking for a technology to automate the deployment of an entire infrastructure, as needed.
Second, does Tailwind Traders need a repeatable and reliable way to deploy its entire infrastructure? Yes, this is exactly what the company needs. Our decision criteria lead us to choose Azure Resource Manager templates (ARM templates) for this scenario.
You could use Azure PowerShell or the Azure CLI, but these scripting technologies have significant limitations when it comes to deploying infrastructure. ARM templates can help overcome these limitations.
The third decision criterion assumes that you need to write a script by using imperative

code. However, when you use ARM templates, you define your infrastructure declaratively by using JSON code. In some instances, you still might need imperative code for configuration or clean-up tasks. In these cases, you can trigger the execution of scripts by using either Azure PowerShell or the Azure CLI to perform these tasks.
In this scenario, ARM templates are the correct choice.

From <https://docs.microsoft.com/en-us/learn/modules/management-fundamentals/8-use-azure-resource-manager>

Choose the best Azure serverless technology for your business scenario

Thursday, January 28, 2021 10:40 AM

Examine Azure serverless technologies, and choose the right service for your business scenario.

Overview

From <https://docs.microsoft.com/en-us/learn/paths/az-900-describe-core-solutions-management-tools-azure/>

Introduction

- 1 minute

Serverless computing is a term used to describe an execution environment that's set up and managed for you. You merely specify what you want to happen by writing code or connecting and configuring components in a visual editor, and then specify the actions that trigger your functionality, such as a timer or an HTTP request. Best of all, you never have to worry about an outage, your code can scale instantly to meet demand, and you pay based only on the actual usage of your code.

Tailwind Traders, a traditional brick-and-mortar retailer, has found success selling online. The company sees several opportunities to improve its e-commerce website. For example, it wants to provide more accurate real-time inventory information online to customers who want to visit their local store to purchase an item. The company also wants to respond more proactively to customers who've had a negative experience by providing a new customer-retention program.

Tailwind Traders suspects that serverless computing can help it provide these services, but it needs help to understand which Azure solutions are right for its business scenarios.

In this module, you'll learn about two serverless computing solutions on Azure: Azure Functions and Azure Logic Apps. You'll learn what they are, how they differ, and when you should choose one over the other.

Learning objectives

After completing this module, you'll be able to:

- Choose the serverless computing technology that best addresses your business scenario.

Prerequisites

- An understanding of the concept of orchestration and workflows
- An understanding of the concept of application programming interface (API)
- High-level familiarity with relevant Microsoft products such as Dynamics 365 and Office 365

From <https://docs.microsoft.com/en-us/learn/modules/serverless-fundamentals/1-introduction>

Identify the product options

- 5 minutes

Serverless computing is a cloud-hosted execution environment that runs your code but abstracts the underlying hosting environment. The term *serverless computing* is a misnomer. After all, there *is* a server (or a group of servers) that executes your code or desired functionality.

The key idea is that you're not responsible for setting up or maintaining the server. You don't have to worry about scaling it when there's increased demand, and you don't have to worry about outages. The cloud vendor takes care of all maintenance and scaling concerns for you.

You create an instance of the service, and you add your code. No infrastructure configuration or maintenance is required, or even allowed. You configure your serverless apps to respond to events. An event could be a REST endpoint, a periodic timer, or even a message received from another Azure service. The serverless app runs only when it's triggered by an event. Scaling and performance are handled automatically, and you're billed only for the resources you use. You don't even need to reserve resources.

Serverless computing is ordinarily used to handle *back-end* scenarios. In other words, serverless computing is responsible for sending message from one system to another, or processing messages that were sent from other systems. It's not used for user-facing systems but, rather, it works in the background.

In this module, we'll cover two Azure serverless computing services: Azure Functions and Azure Logic Apps.

Azure Functions

With the Azure Functions service, you can host a single method or function by using a popular programming language in the cloud that runs in response to an event. An example of an event might be an HTTP request, a new message on a queue, or a message on a timer.

Because of its atomic nature, Azure Functions can serve many purposes in an

application's design. Functions can be written in many common programming languages, such as C#, Python, JavaScript, Typescript, Java, and PowerShell.
Azure Functions scales automatically, and charges accrue only when a function is triggered. These qualities make Azure Functions a solid choice when demand is variable. For example, you might be receiving messages from an IoT solution that monitors a fleet of delivery vehicles. You'll likely have more data arriving during business hours. Azure Functions can scale out to accommodate these busier times.
An Azure function is a stateless environment. A function behaves as if it's restarted every time it responds to an event. This feature is ideal for processing incoming data. And if state is required, the function can be connected to an Azure storage account.
Azure Functions can perform orchestration tasks by using an extension called Durable Functions, which allows developers to chain functions together while maintaining state.
The Azure Functions solution is ideal when you're concerned only with the code that's running your service and not the underlying platform or infrastructure. You use Functions most commonly when you need to perform work in response to an event. You do this often via a REST request, timer, or message from another Azure service, and when that work can be completed quickly, within seconds or less.

Azure Logic Apps

Logic Apps is a low-code/no-code development platform hosted as a cloud service. The service helps you automate and orchestrate tasks, business processes, and workflows when you need to integrate apps, data, systems, and services across enterprises or organizations. Logic Apps simplifies how you design and build scalable solutions, whether in the cloud, on-premises, or both. This solution covers app integration, data integration, system integration, enterprise application integration (EAI), and business-to-business (B2B) integration.
Azure Logic Apps is designed in a web-based designer and can execute logic that's triggered by Azure services without you having to write any code. You build an app by linking triggers to actions with connectors. A trigger is an event, such as a timer, that causes an app to execute, a new message to be sent to a queue, or an HTTP request. An action is a task or step that can execute. There are logic actions such as those you would find in most programming languages. Examples of actions include working with variables, decision statements and loops, and tasks that parse and modify data.
To build enterprise integration solutions with Azure Logic Apps, you can choose from a growing gallery of over 200 connectors. The gallery includes services such as Salesforce, SAP, Oracle DB, and file shares.
If you can't find the action or connector you need, you can build your own by using custom code.

What are the differences between these services?

You can call Azure Functions from Azure Logic Apps, and vice versa. The primary difference between the two services is their intent. Azure Functions is a serverless

compute service, and Azure Logic Apps is intended to be a serverless orchestration service. Although you can use Azure Functions to orchestrate a long-running business process that involves various connections, this was not its primary use case when it was designed.
Additionally, the two services are priced differently. Azure Functions pricing is based on the number of executions and the running time of each execution. Logic Apps pricing is based on the number of executions and the type of connectors that it utilizes.

From <https://docs.microsoft.com/en-us/learn/modules/serverless-fundamentals/2-identify-product-options>

Analyze the decision criteria

- 5 minutes

With two viable serverless options, it can be difficult to know which is the best one for the job. In this unit, we'll analyze the criteria that experts employ when they're choosing a serverless service to use for a given business need. Understanding the criteria can also help you better understand the nuanced differences between the products.

Do you need to perform an orchestration across well-known APIs?

As we noted previously, Azure Logic Apps was designed with orchestration in mind, from the web-based visual configurator to the pricing model. Logic Apps excels at connecting a large array of disparate services via their APIs to pass and process data through many steps in a workflow.
It's possible to create the same workflow by using Azure Functions, but it might take a considerable amount of time to research which APIs to call and how to call them. Azure Logic Apps has already componentized these API calls so that you supply only a few details and the details of calling the necessary APIs is abstracted away.

Do you need to execute custom algorithms or perform specialized data parsing and data lookups?

With Azure Functions, you can use the full expressiveness of a programming language in a compact form. This lets you concisely build complex algorithms, or data lookup and parsing operations. You would be responsible for maintaining the code, handling exceptions resiliently, and so on.
Although Azure Logic Apps can perform logic (loops, decisions, and so on), if you have a logic-intensive orchestration that requires a complex algorithm, implementing that algorithm might be more verbose and visually overwhelming.

Do you have existing automated tasks written in an

imperative programming language?

If you already have your orchestration or business logic expressed in C#, Java, Python, or another popular programming language, it might be easier to port your code into the body of an Azure Functions function app than to re-create it by using Azure Logic Apps.

Do you prefer a visual (declarative) workflow or writing (imperative) code?

Ultimately, your choice comes down to whether you prefer to work in a declarative environment or an imperative environment. Developers who have expertise in an imperative programming language might prefer to think about automation and orchestration from an imperative mindset. IT professionals and business analysts might prefer to work in a more visual low-code/no-code (declarative) environment.

From <https://docs.microsoft.com/en-us/learn/modules/serverless-fundamentals/3-analyze-decision-criteria>

Use Azure Functions

- 3 minutes

Data about each product that's sold at Tailwind Traders is packaged as a JSON message and sent to an event hub. The event hub distributes the JSON message to subscribers, which allows various systems to be notified.

Tailwind Traders wants to upgrade its e-commerce site to include real-time inventory tracking. Currently, the website updates product availability nightly at 2:00 AM. A Windows service that's written in C# contains all of the necessary logic to:

- Retrieve the messages.
- Parse the JSON.
- Perform a lookup across multiple databases to find additional product information.
- Potentially, send notifications to the purchasing department so that they can reorder quantities that fall below certain levels.

The Windows service runs in a virtual machine that's hosted on Azure.

Most of the time, this system works fine. However, some products are in high demand, and some products are kept in low quantities at each store. Several times a day, customers drive to a store to pick up an item only to find that it's no longer in stock. Instead of running the algorithm nightly, the company wants to run the inventory updater each time a product is purchased.

Which service should you choose?

Because the Tailwind Traders developers team has already written the logic in C#, it would make sense to copy the relevant C# code from the Windows service and port it to an Azure function. The developers would bind the function to trigger each time a new

message appears on a specific queue.

Why not choose Azure Logic Apps?

It's possible to implement the same logic in Azure Logic Apps. However, because the team has already invested time in building the service in C#, it can use the same code in an Azure function.

From <https://docs.microsoft.com/en-us/learn/modules/serverless-fundamentals/4-use-azure-functions>

Use Azure Logic Apps

- 2 minutes

Tailwind Traders sends its customers an invitation to participate in a customer satisfaction survey randomly after a purchase. Currently, the customer satisfaction results are aggregated, averaged, and charted. However, its customer service department sees an opportunity to reach out proactively to customers who provide low scores and leave comments with a negative sentiment.

Ideally, negative customer satisfaction scores would trigger a customer retention workflow. First, a sentiment analysis would be generated based on the free-form comments, an email would be sent to the customer with an apology and a coupon code, and the message would be routed to the Dynamics 365 customer service team so that it could schedule a follow-up email.

Unfortunately, no Tailwind Traders developer resources are available to take on this project. But the customer service team works with several cloud and IT professionals who might be able to construct a solution.

Which service should you choose?

In this scenario, Azure Logic Apps is likely the best solution. A cloud or IT professional could use existing connectors to perform a sentiment analysis by using the Azure Cognitive Services connector, send an email by using the Office 365 Outlook connector, and create a new record and follow-up email by using the Dynamics 365 customer service connector.

Because Azure Logic Apps is a low-code/no-code service, no developers are needed. A cloud or IT professional should be able to build and support this workflow.

Why not choose Azure Functions?

Although it's possible to build the entire solution by using Azure Functions, this approach might be challenge if no software developers can be committed to this project.

This is an ideal scenario for Azure Logic Apps. Connectors already exist for each of the

steps outlined in the workflow. It would take quite a bit of research, development, and testing for a developer to build a solution that utilizes all these disparate software systems.

From <https://docs.microsoft.com/en-us/learn/modules/serverless-fundamentals/5-use-azure-logic-apps>

Choose the best Azure IoT service for your application

Thursday, January 28, 2021 10:41 AM

Examine Azure IoT services, and choose the right service for your scenario.

Overview

- Introduction 1 min
- Identify the product options 5 min
- Analyze the decision criteria 3 min
- Use IoT Hub 4 min
- Use IoT Central 4 min
- Use Azure Sphere 4 min
- Knowledge check 3 min
- Summary 1 min

From <https://docs.microsoft.com/en-us/learn/paths/az-900-describe-core-solutions-management-tools-azure/>

Introduction

- 1 minute

IoT bridges the physical and digital worlds by enabling devices with sensors and an internet connection to communicate with cloud-based systems via the internet.

Tailwind Traders sees many opportunities to use Azure IoT services across many different facets of their operations, from new product development to logistics and point-of-sale.

In this module, you'll help Tailwind Traders select the right Azure IoT service offering for its business scenarios. By evaluating the services in relation to a set of decision criteria, you'll learn about what the various services do, how they're different or complementary, and when to use one or the other.

Learning objectives

After you've completed this module, you'll be able to:

- Choose the Azure IoT service that best addresses your business scenario.

Prerequisites

- Familiarity with basic computing concepts and terminology
- Familiarity with cloud computing is helpful but not necessary

From <https://docs.microsoft.com/en-us/learn/modules/iot-fundamentals/1-introduction>

Identify the product options

- 5 minutes

IoT enables devices to gather and then relay information for data analysis. Smart devices are equipped with sensors that collect data. A few common sensors that measure attributes of the physical world include:

- Environmental sensors that capture temperature and humidity levels.
- Barcode, QR code, or optical character recognition (OCR) scanners.
- Geo-location and proximity sensors.
- Light, color, and infrared sensors.
- Sound and ultrasonic sensors.
- Motion and touch sensors.
- Accelerometer and tilt sensors.
- Smoke, gas, and alcohol sensors.
- Error sensors to detect when there's a problem with the device.
- Mechanical sensors that detect anomalies or deformations.
- Flow, level, and pressure sensors for measuring gasses and liquids.

By using Azure IoT services, devices that are equipped with these kinds of sensors and that can connect to the internet could send their sensor readings to a specific endpoint in Azure via a message. The message's data is then collected and aggregated, and it can be converted into reports and alerts. Alternately, all devices could be updated with new firmware to fix issues or add new functionality by sending software updates from Azure IoT services to each device.

Let's suppose your company manufactures and operates smart refrigerated vending machines. What kinds of information would you want to monitor? You might want to ensure that:

- Each machine is operating without any errors.
- The machines haven't been compromised.
- The machines' refrigeration systems are keeping their contents within a certain temperature range.
- You're notified when products reach a certain inventory level so you can restock the machines.

If the hardware of your vending machines can collect and send this information in a standard message, the messages each machine sends can be received, stored, organized, and displayed by using Azure IoT services.

The data that's collected from these devices could be combined with Azure AI services to help you predict:

- When machines need proactive maintenance.
- When inventories will need to be replenished and new product ordered from vendors.

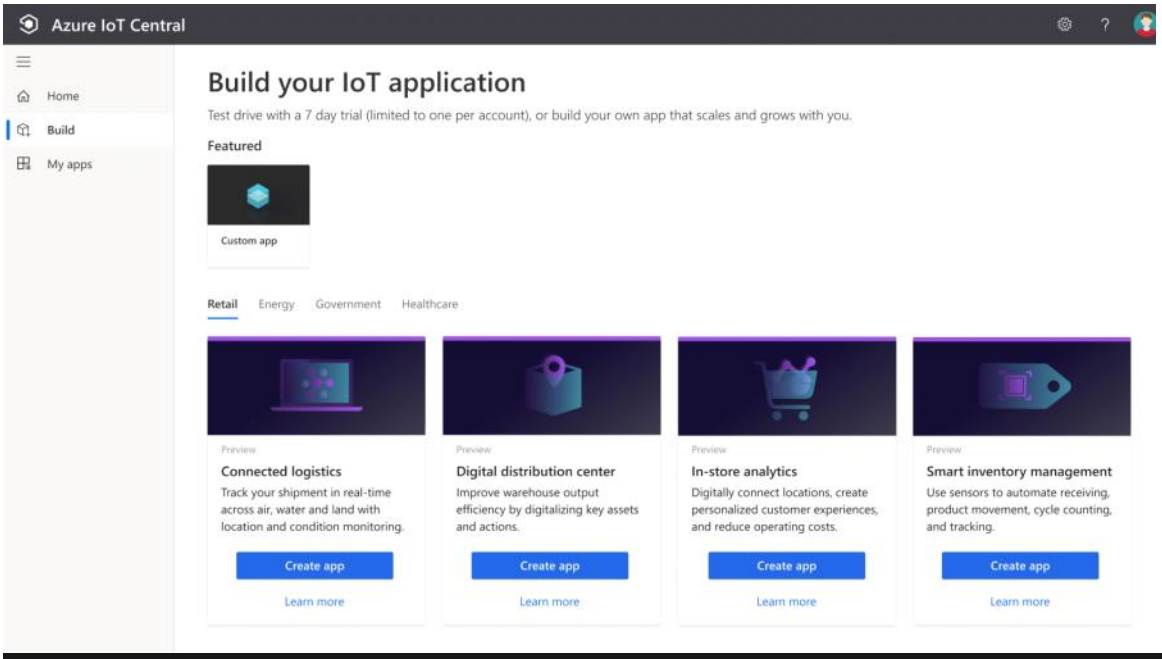
Many services can assist and drive end-to-end solutions for IoT on Azure.

Azure IoT Hub

Azure IoT Hub is a managed service that's hosted in the cloud and that acts as a central message hub for bi-directional communication between your IoT application and the devices it manages. You can use Azure IoT Hub to build IoT solutions with reliable and secure communications between millions of IoT devices and a cloud-hosted solution back end. You can connect virtually any device to your IoT hub.
The IoT Hub service supports communications both from the device to the cloud and from the cloud to the device. It also supports multiple messaging patterns, such as device-to-cloud telemetry, file upload from devices, and request-reply methods to control your devices from the cloud. After an IoT hub receives messages from a device, it can route that message to other Azure services.
From a cloud-to-device perspective, IoT Hub allows for *command and control*. That is, you can have either manual or automated remote control of connected devices, so you can instruct the device to open valves, set target temperatures, restart stuck devices, and so on.
IoT Hub monitoring helps you maintain the health of your solution by tracking events such as device creation, device failures, and device connections.

Azure IoT Central

Azure IoT Central builds on top of IoT Hub by adding a dashboard that allows you to connect, monitor, and manage your IoT devices. The visual user interface (UI) makes it easy to quickly connect new devices and watch as they begin sending telemetry or error messages. You can watch the overall performance across all devices in aggregate, and you can set up alerts that send notifications when a specific device needs maintenance. Finally, you can push firmware updates to the device.
To help you get up and running quickly, IoT Central provides starter templates for common scenarios across various industries, such as retail, energy, healthcare, and government. You then customize the design starter templates directly in the UI by choosing from existing themes or creating your own custom theme, setting the logo, and so on. With IoT Central, you can tailor the starter templates for the specific data that's sent from your devices, the reports you want to see, and the alerts you want to send.



You can use the UI to control your devices remotely. This feature allows you to push a software update or modify a property of the device. You can adjust the desired temperature for one or all of your refrigerated vending machines from directly inside of IoT Central.

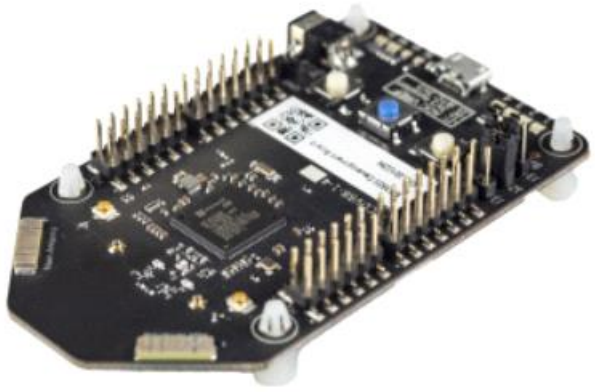
A key part of IoT Central is the use of device templates. By using a device template, you can connect a device without any service-side coding. IoT Central uses the templates to construct the dashboards, alerts, and so on. Device developers still need to create code to run on the devices, and that code must match the device template specification.

Azure Sphere

Azure Sphere creates an end-to-end, highly secure IoT solution for customers that encompasses everything from the hardware and operating system on the device to the secure method of sending messages from the device to the message hub. Azure Sphere has built-in communication and security features for internet-connected devices.

Azure Sphere comes in three parts:

- The first part is the Azure Sphere micro-controller unit (MCU), which is responsible for processing the operating system and signals from attached sensors. The following image displays the Seed Azure Sphere MT3620 Development Kit MCU, one of several different starter kits that are available for prototyping and developing Azure Sphere applications.



- The second part is a customized Linux operating system (OS) that handles communication with the security service and can run the vendor's software.
- The third part is Azure Sphere Security Service, also known as AS3. Its job is to make sure that the device has not been maliciously compromised. When the device attempts to connect to Azure, it first must authenticate itself, per device, which it does by using certificate-based authentication. If it authenticates successfully, AS3 checks to ensure that the device hasn't been tampered with. After it has established a secure channel of communication, AS3 pushes any OS or approved customer-developed software updates to the device.

After the Azure Sphere system has validated the authenticity of the device and authenticated it, the device can interact with other Azure IoT services by sending telemetry and error information.

From <https://docs.microsoft.com/en-us/learn/modules/iot-fundamentals/2-identify-product-options>

Analyze the decision criteria

- 3 minutes

In this unit, we'll analyze the criteria that experts employ when they decide which IoT service to use for a given business need. Understanding the criteria can also help you better understand the nuanced differences between each product.

Is it critical to ensure that the device is not compromised?

No manufacturers or customers want their devices to be maliciously compromised and used for nefarious purposes, but it's more critical to ensure the integrity of an ATM than, say, a washing machine. When security is a critical consideration in your product's design, the best product option is Azure Sphere, which provides a comprehensive end-to-end solution for IoT devices.

As we mentioned in the previous unit, Azure Sphere ensures a secure channel of communication between the device and Azure by controlling everything from the hardware to the operating system and the authentication process. This ensures that the integrity of the device is uncompromised. After a secure channel is established,

messages can be received from the device securely, and messages or software updates can be sent to the device remotely.

Do I need a dashboard for reporting and management?

Your next decision will be the level of services you require from your IoT solution. If you merely want to connect to your remote devices to receive telemetry and occasionally push updates, and you don't need any reporting capabilities, you might prefer to implement Azure IoT Hub by itself. Your programmers can still create a customized set of management tools and reports by using the IoT Hub RESTful API.
However, if you want a pre-built customizable user interface with which you can view and control your devices remotely, you might prefer to start with IoT Central. With this solution, you can control a single device or all devices at once, and you can set up alerts for certain conditions, such as a device failure.
IoT Central integrates with many different Azure products, including IoT Hub, to create a dashboard with reports and management features. The dashboard is based on starter templates for common industry and usage scenarios. You can use the dashboard that's generated by the starter template as is or customize it to suit your needs. You can have multiple dashboards and target them at a variety of users.

From <https://docs.microsoft.com/en-us/learn/modules/iot-fundamentals/3-analyze-decision-criteria>

Use IoT Hub

- 4 minutes

The Tailwind Traders senior leadership team has decided to partner with a leading appliance manufacture to create an exclusive, high-end brand that promises a preemptive maintenance service agreement. This unique feature would differentiate Tailwind Traders appliances in a crowded, competitive market. The feature also makes the brand lucrative, because a yearly subscription would be required. To build a strong brand reputation, the appliances will send telemetry information to a centralized location, where it can be analyzed and maintenance can be scheduled.
The devices will not require remote control. They will merely be sending their telemetry data for analysis and pro-active maintenance.
Because Tailwind Traders already has software in place for managing appliance maintenance requests, the company wants to integrate all functionality into this existing system.

Which service should you choose?

Let's apply the decision criteria from the previous unit.
First, is it critical to ensure that the device or, in this case, each appliance, isn't compromised? It's preferable, but not critical, that the devices aren't compromised. The

worst that could happen is that a hacker reads the current temperature of the customer's refrigerator or the number of loads of laundry the washing machine has completed.
Even if the customer calls and reports strange behavior with their appliance, a technician could reset or replace the microcontroller. It might not warrant the extra expense or engineering resources that would be required to employ Azure Sphere.
Second decision criterion: do I need a dashboard for reporting and management? In this case, no. Tailwind Traders wants to integrate the telemetry data and all other functionality into an existing maintenance request system. In this case, Azure IoT Central is not required.
So, given the responses to the decision criteria, Azure IoT Hub is the best choice in this scenario.

Why not use Azure IoT Central?

Azure IoT Central provides a dashboard that allows companies to manage IoT devices individually and an aggregate, view reports, and set up error notifications via a GUI. But, in this scenario, Tailwind Traders wants to integrate the telemetry it collects and other analysis functionality into an existing software application. Furthermore, the company's appliances will be collecting data via sensors only and don't need the ability to update settings or software remotely. Therefore, the company doesn't need Azure IoT Central.

Why not use Azure Sphere?

Azure Sphere provides a complete solution for scenarios where security is critical. In this scenario, security is preferred but not critical. The appliances can't be updated with new software remotely. The sensors merely report usage data. As a result, Azure Sphere isn't necessary.

From <https://docs.microsoft.com/en-us/learn/modules/iot-fundamentals/4-use-iot-hub>

Use IoT Central

- 4 minutes

Tailwind Traders owns a fleet of delivery vehicles that transport products from warehouses to distribution centers, and from distribution centers to stores and homes. The company is looking for a complete logistics solution that takes data sent from an onboard vehicle computer and turns it into actionable information.
Furthermore, shipments can be outfitted with sensors from a third-party vendor to collect and monitor ambient conditions. These sensors can collect information such as the temperature, humidity, tilt, shock, light, and the location of a shipment.
A few goals of this logistics system include:

- Shipment monitoring with real-time tracing and tracking.
- Shipment integrity with real-time ambient condition monitoring.

- Security from theft, loss, or damage of shipments.
- Geo-fencing, route optimization, fleet management, and vehicle analytics.
- Forecasting for predictable departure and arrival of shipments.

The company would prefer a pre-built solution to collect the sensor and vehicle computer data, and provide a graphical user interface that displays reports about shipments and vehicles.

Which service should you choose?

Here again, apply the decision criteria that you learned about earlier.
First, is it critical to ensure that the device or, in this case, each appliance, isn't compromised? Ideally, each sensor and vehicle computer would be impervious to interference. However, security was not mentioned as a critical concern at this point. The vehicle computers and sensors are built by a third-party vendor and, unless Tailwind Traders wants to manufacture its own devices (which they don't), the company will be forced to use hardware that's already available.
Second, does Tailwind Traders need a dashboard for reporting and management? Yes, a reporting and management dashboard is a requirement.
Based on these responses to the decision criteria, Azure IoT Central is the best choice in this scenario. The Connected Logistics starter template provides an out-of-box dashboard that will satisfy many of these requirements. This dashboard is preconfigured to showcase the critical logistics device operations activity. Admittedly, the dashboard might need to be reconfigured to remove sea vessel gateways, but the truck gateway functionality would be almost exactly what Tailwind Traders needs.

Why not use IoT Hub?

If Tailwind Traders uses IoT Central, the company would actually be using an IoT hub that's preconfigured for its specific needs by the Connected Logistics starter template. Otherwise, the company would need to do a lot of custom development to build its own cloud-based dashboards and management systems on top of Azure IoT Hub.

Why not use Azure Sphere?

Azure Sphere provides a complete solution for scenarios where security is critical. In this scenario, security is ideal, but not a critical priority. Although Azure Sphere provides an end-to-end solution that includes hardware, Tailwind Traders will use hardware from a third-party vendor. So, in this scenario, Azure Sphere is not necessary.

From <https://docs.microsoft.com/en-us/learn/modules/iot-fundamentals/5-use-iot-central>

Use Azure Sphere

- 4 minutes

Tailwind Traders wants to implement a touchless point-of-sale solution for self-checkout. The self-checkout terminals should be, above all else, secure. Each terminal must be impervious to malicious code that could create fraudulent transactions, force the company to take the systems offline during a heavy shopping period, or send transactional data to a spying organization. The terminals should also report back vital information on the company's health and allow secure updates to its software remotely.
After reviewing many possible solutions during a request for proposal process, Tailwind Traders decides that it needs features that vendors have yet to implement. Instead of using an existing solution, the company decides to work with a leading engineering firm that specializes in IoT solutions. This approach allows the company to build a uniquely secure terminal that gives it a retail platform to build on going forward.
Although most of the company's focus is on the terminal itself, Tailwind Traders realizes that it wants a solution that can help it make sense of all the data that will be generated by these terminals across all of its retail stores. And it wants an easy way to push software updates to its terminals.

Which service should you choose?

Again, apply the decision criteria as you've been doing.
First, is it critical to ensure that the device or, in this case, each point-of-sale terminal, is not compromised? Absolutely. Device security is the primary requirement.
Next, does Tailwind Traders need a dashboard for reporting and management? Yes, the company requires a reporting and management dashboard.
So, given the responses to the decision criteria, the IoT engineering firm will build a platform on top of both Azure IoT Central and Azure Sphere. Even though no specific starter template is available in Azure IoT Central for this scenario, one can easily be adapted to accommodate the kinds of reports the company wants to see and the management operations it wants to perform.

Why not choose IoT Hub?

By using IoT Central, Tailwind Traders would actually be using Azure IoT Hub behind the scenes as well.

From <https://docs.microsoft.com/en-us/learn/modules/iot-fundamentals/6-use-azure-sphere>

Part 4: Describe general security and network security features

Thursday, January 28, 2021 10:45 AM

Protect against security threats on Azure

Thursday, January 28, 2021 10:45 AM

Learn how Azure can help you protect the workloads that you run both in the cloud and in your on-premises datacenter.

Overview

- Introduction 1 min
- Protect against security threats by using Azure Security Center 4 min
- Detect and respond to security threats by using Azure Sentinel 4 min
- Store and manage secrets by using Azure Key Vault 3 min
- Exercise - Manage a password in Azure Key Vault 5 min
- Host your Azure virtual machines on dedicated physical servers by using Azure Dedicated Host 2 min
- Knowledge check 2 min
- Summary 2 min

From <https://docs.microsoft.com/en-us/learn/paths/az-900-describe-general-security-network-security-features/>

Introduction

- 1 minute

In this module, you'll learn about some of the security tools that can help keep your infrastructure and data safe when you work in the cloud.

Security is a small word for a significant concept. There are so many factors to consider in order to protect your applications and your data. How does Azure help you protect workloads that you run in the cloud and in your on-premises datacenter?

Meet Tailwind Traders

Tailwind Traders is a fictitious home improvement retailer. It operates retail hardware stores across the globe and online.

Tailwind Traders specializes in competitive pricing, fast shipping, and a large range of items. It's looking at cloud technologies to improve business operations and support growth into new markets. By moving to the cloud, the company plans to enhance its shopping experience to further differentiate itself from competitors.

How will Tailwind Traders run securely in the cloud and in the datacenter?

Tailwind Traders runs a mix of workloads on Azure and in its datacenter.
The company needs to ensure that all of its systems meet a minimum level of security and that its information is protected from attacks. The company also needs a way to collect and act on security events from across its digital estate.
Let's explore how Tailwind Traders can use some of the tools and features in Azure as part of its overall security strategy.

Learning objectives

After completing this module, you'll be able to:

- Strengthen your security posture and protect against threats by using Azure Security Center.
- Collect and act on security data from many different sources by using Azure Sentinel.
- Store and access sensitive information such as passwords and encryption keys securely in Azure Key Vault.
- Manage dedicated physical servers to host your Azure VMs for Windows and Linux by using Azure Dedicated Host.

Prerequisites

- You should be familiar with basic computing concepts and terminology.
- Familiarity with cloud computing is helpful but isn't necessary.

From <https://docs.microsoft.com/en-us/learn/modules/protect-against-security-threats-azure/1-introduction>

Protect against security threats by using Azure Security Center

- 4 minutes

Tailwind Traders is broadening its use of Azure services. It still has on-premises workloads with current security-related configuration best practices and business procedures. How does the company ensure that all of its systems meet a minimum level of security and that its information is protected from attacks?
Many Azure services include built-in security features. Tools on Azure can also help Tailwind Traders with this requirement. Let's start by looking at Azure Security Center.

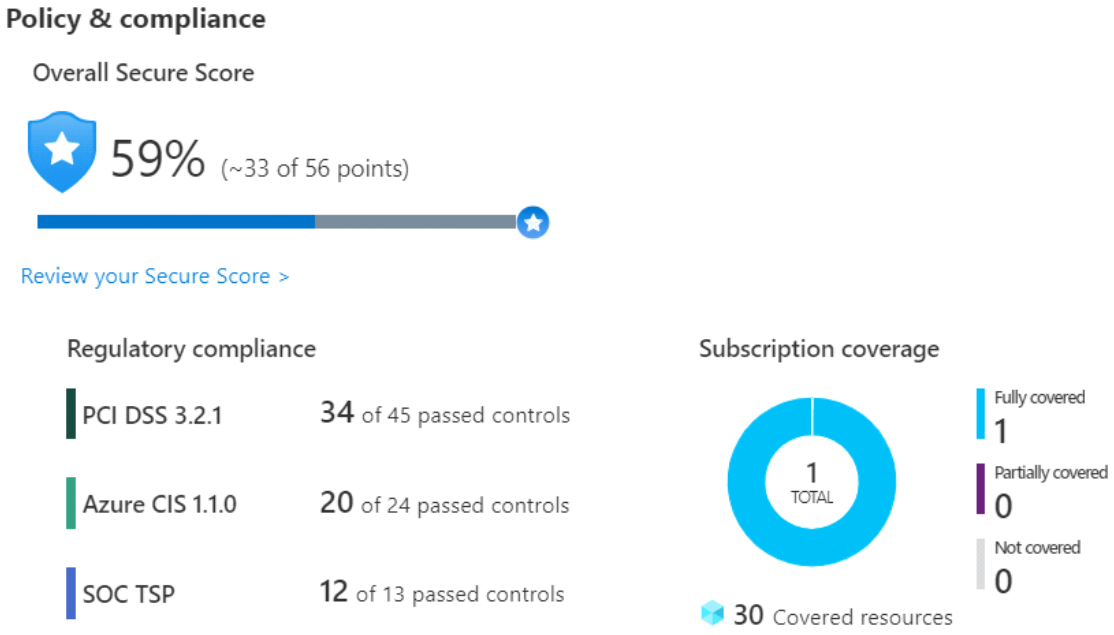
What's Azure Security Center?

Azure Security Center is a monitoring service that provides visibility of your security posture across all of your services, both on Azure and on-premises. The term *security posture* refers to cybersecurity policies and controls, as well as how well you can predict, prevent, and respond to security threats.
Security Center can:

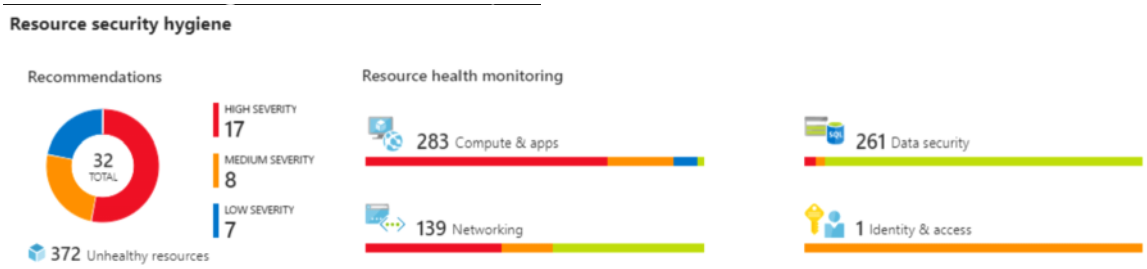
- Monitor security settings across on-premises and cloud workloads.
- Automatically apply required security settings to new resources as they come online.
- Provide security recommendations that are based on your current configurations, resources, and networks.
- Continuously monitor your resources and perform automatic security assessments to identify potential vulnerabilities before those vulnerabilities can be exploited.
- Use machine learning to detect and block malware from being installed on your virtual machines (VMs) and other resources. You can also use *adaptive application controls* to define rules that list allowed applications to ensure that only applications you allow can run.
- Detect and analyze potential inbound attacks and investigate threats and any post-breach activity that might have occurred.
- Provide just-in-time access control for network ports. Doing so reduces your attack surface by ensuring that the network only allows traffic that you require at the time that you need it to.

Understand your security posture

Tailwind Traders can use Security Center to get a detailed analysis of different components in its environment. Because the company's resources are analyzed against the security controls of any governance policies it has assigned, it can view its overall regulatory compliance from a security perspective all from one place.
Here's an example of what you might see in Azure Security Center:

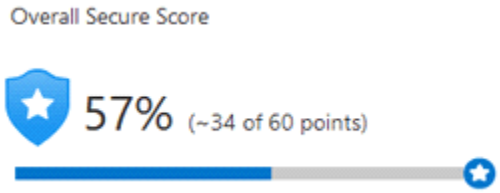


Let's say that Tailwind Traders must comply with the Payment Card Industry's Data Security Standard (PCI DSS). This report shows that the company has resources that it needs to remediate.
In the Resource security hygiene section, Tailwind Traders can see the health of its resources from a security perspective. To help prioritize remediation actions, recommendations are categorized as low, medium, and high. Here's an example:



What's secure score?

Secure score is a measurement of an organization's security posture.
Secure score is based on *security controls*, or groups of related security recommendations. Your score is based on the percentage of security controls that you satisfy. The more security controls you satisfy, the higher the score you receive. Your score improves when you remediate all of the recommendations for a single resource within a control.
Here's an example from the Azure portal showing a score of 57 percent, or 34 out of 60 points:



Following the secure score recommendations can help protect your organization from threats. From a centralized dashboard in Azure Security Center, organizations can monitor and work on the security of their Azure resources like identities, data, apps, devices, and infrastructure.
Secure score helps you:

- Report on the current state of your organization's security posture.
- Improve your security posture by providing discoverability, visibility, guidance, and control.
- Compare with benchmarks and establish key performance indicators (KPIs).

Protect against threats

Security Center includes advanced cloud defense capabilities for virtual machines, network security, and file integrity. Let's look at how some of these capabilities apply to Tailwind Traders.

- Just-in-time VM access
  Tailwind Traders will configure just-in-time access to VMs. This access blocks traffic by default to specific network ports of virtual machines, but allows traffic for a specified time when an administrator requests and approves it.
- Adaptive application controls
  Tailwind Traders can control which applications are allowed to run on its virtual machines. In the background, Security Center uses machine learning to look at the processes running on a virtual machine. It creates exception rules for each resource group that holds the virtual machines and provides recommendations. This process provides alerts that inform the company about unauthorized applications that are running on its VMs.
- Adaptive network hardening

Security Center can monitor the internet traffic patterns of the VMs and compare those patterns with the company's current network security group (NSG) settings. From there, Security Center can make recommendations on whether the NSGs should be locked down further and provide remediation steps.

- File integrity monitoring
  Tailwind Traders can also configure the monitoring of changes to important files on both Windows and Linux, registry settings, applications, and other aspects that might indicate a security attack.

Respond to security alerts

Tailwind Traders can use Security Center to get a centralized view of all of its security alerts. From there, the company can dismiss false alerts, investigate them further, remediate alerts manually, or use an automated response with a *workflow automation*.
Workflow automation uses Azure Logic Apps and Security Center connectors. The logic app can be triggered by a threat detection alert or by a Security Center recommendation, filtered by name or by severity. You can then configure the logic app to run an action such as sending an email or posting a message to a Microsoft Teams channel.

From <https://docs.microsoft.com/en-us/learn/modules/protect-against-security-threats-azure/2-protect-threats-security-center>

Detect and respond to security threats by using Azure Sentinel

- 4 minutes

Security management on a large scale can benefit from a dedicated security information and event management (SIEM) system. A SIEM system aggregates security data from many different sources (as long as those sources support an open-standard logging format). It also provides capabilities for threat detection and response.
Azure Sentinel is Microsoft's cloud-based SIEM system. It uses intelligent security analytics and threat analysis.

Azure Sentinel capabilities

Azure Sentinel enables you to:

- Collect cloud data at scale
  Collect data across all users, devices, applications, and infrastructure, both on-premises and from multiple clouds.
- Detect previously undetected threats
  Minimize false positives by using Microsoft's comprehensive analytics and threat intelligence.
- Investigate threats with artificial intelligence
  Examine suspicious activities at scale, tapping into years of cybersecurity experience from Microsoft.

- Respond to incidents rapidly
  Utilize built-in orchestration and automation of common tasks.

Connect your data sources

Tailwind Traders decides to explore the capabilities of Azure Sentinel. First, the company identifies and connects its data sources.
Azure Sentinel supports a number of data sources, which it can analyze for security events. These connections are handled by built-in connectors or industry-standard log formats and APIs.

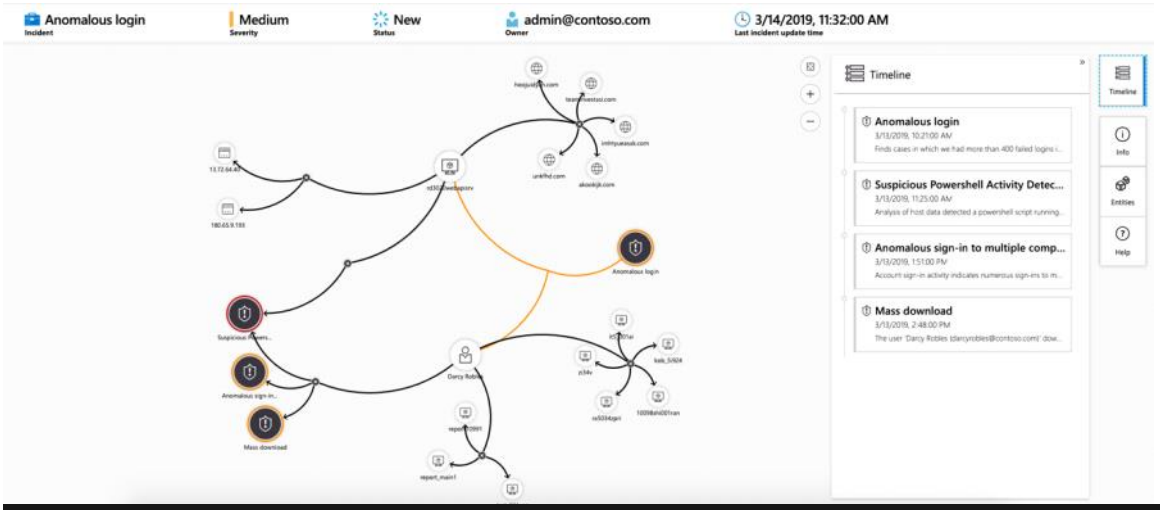
- Connect Microsoft solutions
  Connectors provide real-time integration for services like Microsoft Threat Protection solutions, Microsoft 365 sources (including Office 365), Azure Active Directory, and Windows Defender Firewall.
- Connect other services and solutions
  Connectors are available for common non-Microsoft services and solutions, including AWS CloudTrail, Citrix Analytics (Security), Sophos XG Firewall, VMware Carbon Black Cloud, and Okta SSO.
- Connect industry-standard data sources
  Azure Sentinel supports data from other sources that use the Common Event Format (CEF) messaging standard, Syslog, or REST API.

Detect threats

Tailwind Traders needs to be notified when something suspicious occurs. It decides to use both built-in analytics and custom rules to detect threats.
Built in analytics use templates designed by Microsoft's team of security experts and analysts based on known threats, common attack vectors, and escalation chains for suspicious activity. These templates can be customized and search across the environment for any activity that looks suspicious. Some templates use machine learning behavioral analytics that are based on Microsoft proprietary algorithms.
Custom analytics are rules that you create to search for specific criteria within your environment. You can preview the number of results that the query would generate (based on past log events) and set a schedule for the query to run. You can also set an alert threshold.

Investigate and respond

When Azure Sentinel detects suspicious events, Tailwind Traders can investigate specific alerts or *incidents* (a group of related alerts). With the investigation graph, the company can review information from entities directly connected to the alert and see common exploration queries to help guide the investigation.
Here's an example that shows what an investigation graph looks like in Azure Sentinel:



The company will also use Azure Monitor Workbooks to automate responses to threats. For example, it can set an alert that looks for malicious IP addresses that access the network and create a workbook that does the following steps:

1. When the alert is triggered, open a ticket in the IT ticketing system.
2. Send a message to the security operations channel in Microsoft Teams or Slack to make sure the security analysts are aware of the incident.
3. Send all of the information in the alert to the senior network admin and to the security admin. The email message includes two user option buttons: Block or Ignore.

When an admin chooses Block, the IP address is blocked in the firewall and the user is disabled in Azure Active Directory. When an admin chooses Ignore, the alert is closed in Azure Sentinel and the incident is closed in the IT ticketing system.
The workbook continues to run after it receives a response from the admins.
Workbooks can be run manually or automatically when a rule triggers an alert.

From <https://docs.microsoft.com/en-us/learn/modules/protect-against-security-threats-azure/3-detect-respond-threats-sentinel>

Store and manage secrets by using Azure Key Vault

- 3 minutes

As Tailwind Traders builds its workloads in the cloud, it needs to carefully handle sensitive information such as passwords, encryption keys, and certificates. This information needs to be available for an application to function, but it might allow an unauthorized person access to application data.
Azure Key Vault is a centralized cloud service for storing an application's secrets in a single, central location. It provides secure access to sensitive information by providing access control and logging capabilities.

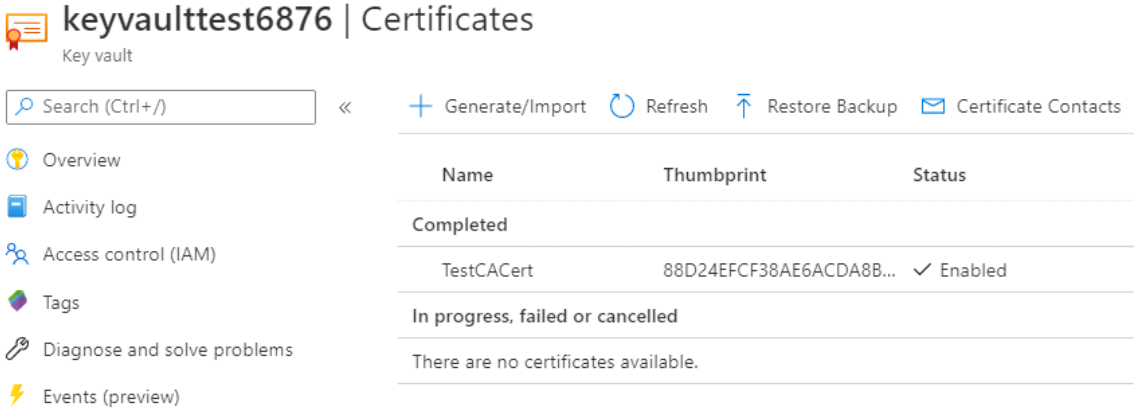
What can Azure Key Vault do?

Azure Key Vault can help you:

- Manage secrets
  You can use Key Vault to securely store and tightly control access to tokens, passwords, certificates, API keys, and other secrets.

- Manage encryption keys
  You can use Key Vault as a key management solution. Key Vault makes it easier to create and control the encryption keys that are used to encrypt your data.
- Manage SSL/TLS certificates
  Key Vault enables you to provision, manage, and deploy your public and private Secure Sockets Layer / Transport Layer Security (SSL/TLS) certificates for both your Azure resources and your internal resources.
- Store secrets backed by hardware security modules (HSMs)
  These secrets and keys can be protected either by software or by FIPS 140-2 Level 2 validated HSMs.

Here's an example that shows a certificate used for testing in Key Vault.



You'll add a secret to Key Vault later in this module.

What are the benefits of Azure Key Vault?

The benefits of using Key Vault include:

- Centralized application secrets
  Centralizing the storage for your application secrets enables you to control their distribution and reduces the chances that secrets are accidentally leaked.
- Securely stored secrets and keys
  Azure uses industry-standard algorithms, key lengths, and HSMs. Access to Key Vault requires proper authentication and authorization.
- Access monitoring and access control
  By using Key Vault, you can monitor and control access to your application secrets.
- Simplified administration of application secrets
  Key Vault makes it easier to enroll and renew certificates from public certificate authorities (CAs). You can also scale up and replicate content within regions and use standard certificate management tools.
- Integration with other Azure services
  You can integrate Key Vault with storage accounts, container registries, event hubs, and many more Azure services. These services can then securely reference the secrets stored in Key Vault.

From <https://docs.microsoft.com/en-us/learn/modules/protect-against-security-threats-azure/4-manage-secrets-key-vault>

Exercise - Manage a password in Azure Key Vault

- 5 minutes

This module requires a sandbox to complete. A sandbox gives you access to free resources. Your personal subscription will not be charged. The sandbox may only be used to complete training on Microsoft Learn. Use for any other reason is prohibited, and may result in permanent loss of access to the sandbox.

Sign in to activate sandbox

In this exercise, you add a password to Azure Key Vault. A password is an example of sensitive information that you need to protect. You then read the password from Azure Key Vault to verify that the password is accessible.

In practice, there are several ways to add secrets to and read secrets from Key Vault. You can use the Azure portal, the Azure CLI, or Azure PowerShell. By using your favorite programming language, your applications can also securely access the secrets that they need.

Here, you create a secret in Key Vault by using the Azure portal. You then access the secret from the portal and from the Azure CLI in Azure Cloud Shell.

The Azure CLI is a way to work with Azure resources from the command line or from scripts. Cloud Shell is a browser-based shell experience to manage and develop Azure resources. Think of Cloud Shell as an interactive console that runs in the cloud.

Create a key vault

1. Go to the Azure portal .
2. On the Azure portal menu or from the Home page, select Create a resource.
3. From the search bar, enter Key Vault. Then select Key Vault from the results.
4. On the Key Vault pane, select Create.
5. On the Create key vault pane, fill in these settings:

   Note

   Replace *NNN* with a series of numbers. This helps ensure that the name of your key vault is unique.

Setting	Value
Subscription	Concierge Subscription
Resource group	[sandbox resource group name]
Key vault name	my-kv-NNN

   TABLE 1

   Leave the other settings at their current values.
6. Select Review + create, and then select Create.

   Wait for the creation process to finish.
7. Select Go to resource.
8. Note some of the details about your key vault.

   For example, the Vault URI field shows the URI that your application can use to access your vault from the REST API.

   Here's an example for a key vault that's named my-kv-1234:

Resource group (change)	: learn-acc1d54a-2366-42c2-ad35-10afd87825f7	DNS Name	: https://my-kv-1234.vault.azure.net/
Location	: East US	Sku (Pricing tier)	: Standard
Subscription (change)	: Concierge Subscription	Directory ID	: 604c1504-c6a3-4080-81aa-b33091104187
Subscription ID	: 7083c8f7-299c-4dd7-9297-7c6c76acb8a0	Directory Name	: Microsoft Learn Sandbox
		Soft-delete	: Enabled
		Purge protection	: Disabled

9. As an optional step, under Settings, examine some of the other settings. Although they're initially empty, here you'll find places where you can store keys, secrets, and certificates.
   Note
   Your Azure subscription is the only one that's authorized to access this vault. Under Settings, the Access policies section enables you to configure access to the vault.

Add a password to the key vault

1. Under Settings, select Secrets, and then select Generate/Import.
2. On the Create a secret pane, fill in these settings:

Setting	Value
Upload options	Manual
Name	MyPassword
Value	hVFkk96

TABLE 2

Leave the other settings at their default values. But notice that you can specify properties such as the activation date and the expiration date. You can also disable access to the secret.

3. Select Create.

Show the password

Here, you access the password from Key Vault two times. First, you access it from the Azure portal. Then you access it from the Azure CLI.

1. From your Key Vault, select MyPassword.
   You see that the current version is enabled.
2. Select the current version.
   Under Secret Identifier, you see a URI that you can now use with applications to access the secret. Remember, only authorized applications can access this secret.
3. Select Show Secret Value.

4. From the Cloud Shell pane to the side of the screen, run this command.
   Note
   If you're not familiar with the Azure CLI, just follow along.
   Azure CLICopy

```
az keyvault secret show \
  --name MyPassword \
  --vault-name $(az keyvault list --query [0].name --output tsv) \
  --query value \
  --output tsv
```

You see the password in the output:

OutputCopy

```
hVFkk96
```

Good work! At this point, you have a key vault that contains a password secret that's securely stored for use with your applications.

Clean up

The sandbox automatically cleans up your resources when you're finished with this module. When you're working in your own subscription, it's a good idea at the end of a project to identify whether you still need the resources you created. Resources left running can cost you money. You can delete resources individually or delete the resource group to delete the entire set of resources.

Next unit: Host your Azure virtual machines on dedicated physical servers by using Azure Dedicated Host

From <https://docs.microsoft.com/en-us/learn/modules/protect-against-security-threats-azure/5-manage-password-key-vault>

Host your Azure virtual machines on dedicated physical servers by using Azure Dedicated Host

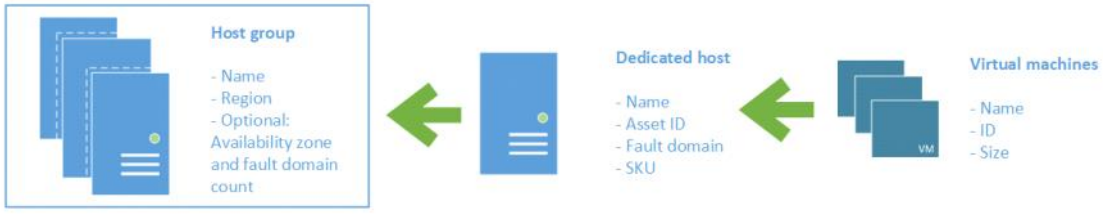
- 2 minutes

On Azure, virtual machines (VMs) run on shared hardware that Microsoft manages. Although the underlying hardware is shared, your VM workloads are isolated from workloads that other Azure customers run.

Some organizations must follow regulatory compliance that requires them to be the only customer using the physical machine that hosts their virtual machines. Azure Dedicated Host provides dedicated physical servers to host your Azure VMs for Windows and Linux.

Here's a diagram that shows how virtual machines relate to dedicated hosts and host groups.

A *dedicated host* is mapped to a physical server in an Azure datacenter. A *host group* is a collection of dedicated hosts.



What are the benefits of Azure Dedicated Host?

Azure Dedicated Host:

- Gives you visibility into, and control over, the server infrastructure that's running your Azure VMs.
- Helps address compliance requirements by deploying your workloads on an isolated server.
- Lets you choose the number of processors, server capabilities, VM series, and VM sizes within the same host.

Availability considerations for Dedicated Host

After a dedicated host is provisioned, Azure assigns it to the physical server in Microsoft's cloud datacenter.
For high availability, you can provision multiple hosts in a *host group* and deploy your virtual machines across this group. VMs on dedicated hosts can also take advantage of *maintenance control*. This feature enables you to control when regular maintenance updates occur, within a 35-day rolling window.

Pricing considerations

You're charged per dedicated host, independent of how many virtual machines you deploy to it. The host price is based on the VM family, type (hardware size), and region.
Software licensing, storage, and network usage are billed separately from the host and VMs. For more information. see Azure Dedicated Host pricing .

From <https://docs.microsoft.com/en-us/learn/modules/protect-against-security-threats-azure/6-host-virtual-machines-dedicated-hosts>

Secure network connectivity on Azure

Thursday, January 28, 2021 10:47 AM

Learn about the Azure services you can use to help ensure that your network is safe, secure, and trusted.

Overview

- Introduction 1 min
- What is defense in depth? 6 min
- Protect virtual networks by using Azure Firewall 3 min
- Protect from DDoS attacks by using Azure DDoS Protection 3 min
- Filter network traffic by using network security groups 2 min
- Exercise - Configure network access to a VM by using a network security group 10 min
- Combine Azure services to create a complete network security solution 3 min
- Knowledge check 3 min
- Summary 1 min

From <https://docs.microsoft.com/en-us/learn/paths/az-900-describe-general-security-network-security-features/>

Introduction

- 1 minute

Every application and service, whether on-premises or in the cloud, needs to be designed with security in mind. There's too much at risk. For example, a denial-of-service attack might prevent customers from reaching your website or services and block you from doing business. Or, your website might be defaced, causing damage to your reputation. A data breach would be even worse, because it can ruin hard-earned trust while causing significant personal and financial harm.

Meet Tailwind Traders

Tailwind Traders is a fictitious home improvement retailer. It operates retail hardware stores across the globe and online.

Tailwind Traders specializes in competitive pricing, fast shipping, and a large range of items. It's looking at cloud technologies to improve business operations and support growth into new markets. By moving to the cloud, the company plans to enhance its shopping experience to further differentiate itself from competitors.

How will Tailwind Traders secure its networks?

As Tailwind Traders moves to the cloud, it needs to evaluate its security needs before it can deploy a single line of code to production.
Although security must be considered at every layer in the company's applications (all the way from the physical servers to the application data), some factors relate specifically to the network configuration and network traffic of cloud-based workloads.
In this module, you'll focus on the network security capabilities in Azure and review how they help you secure your solutions in the cloud, based on your business needs.

Learning objectives

After completing this module, you'll be able to:

- Identify the layers that make up a *defense in depth* strategy.
- Explain how Azure Firewall enables you to control what traffic is allowed on the network.
- Configure network security groups to filter network traffic to and from Azure resources within a Microsoft Azure virtual network.
- Explain how Azure DDoS Protection helps protect your Azure resources from DDoS attacks.

Prerequisites

- You should be familiar with basic computing concepts and terminology.
- Familiarity with cloud computing is helpful but isn't necessary.

From <https://docs.microsoft.com/en-us/learn/modules/secure-network-connectivity-azure/1-introduction>

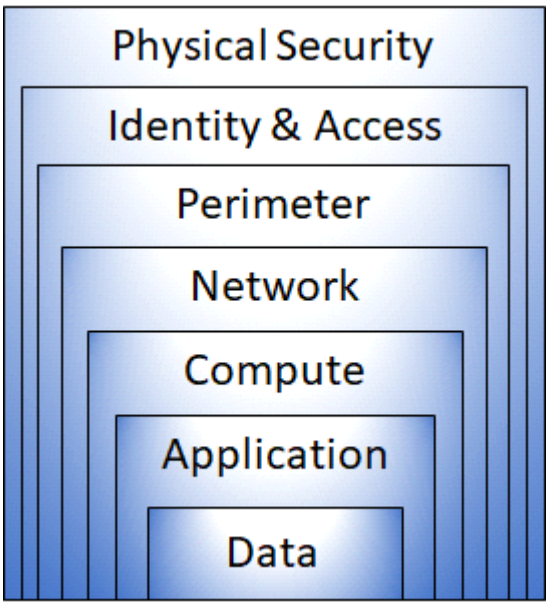
What is defense in depth?

- 6 minutes

Tailwind Traders currently runs its workloads on-premises, in its datacenter. Running on-premises means that the company is responsible for all aspects of security, from physical access to buildings all the way down to how data travels in and out of the network. The company wants to know how its current defense-in-depth strategy compares to running in the cloud.
The objective of *defense in depth* is to protect information and prevent it from being stolen by those who aren't authorized to access it.
A defense-in-depth strategy uses a series of mechanisms to slow the advance of an attack that aims at acquiring unauthorized access to data.

Layers of defense in depth

You can visualize defense in depth as a set of layers, with the data to be secured at the center.



Each layer provides protection so that if one layer is breached, a subsequent layer is already in place to prevent further exposure. This approach removes reliance on any single layer of protection. It slows down an attack and provides alert telemetry that security teams can act upon, either automatically or manually.

Here's a brief overview of the role of each layer:

- The *physical security* layer is the first line of defense to protect computing hardware in the datacenter.
- The *identity and access* layer controls access to infrastructure and change control.
- The *perimeter* layer uses distributed denial of service (DDoS) protection to filter large-scale attacks before they can cause a denial of service for users.
- The *network* layer limits communication between resources through segmentation and access controls.
- The *compute* layer secures access to virtual machines.
- The *application* layer helps ensure that applications are secure and free of security vulnerabilities.
- The *data* layer controls access to business and customer data that you need to protect.

These layers provide a guideline for you to help make security configuration decisions in all of the layers of your applications.

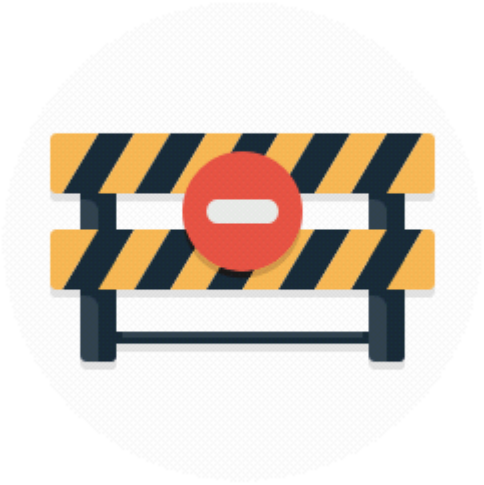
Azure provides security tools and features at every level of the defense-in-depth concept. Let's take a closer look at each layer:

Physical security
Physically securing access to buildings and controlling access to computing hardware within the datacenter are the first line of defense.
With physical security, the intent is to provide physical safeguards against access to assets. These safeguards ensure that other layers can't be bypassed, and loss or theft is handled appropriately. Microsoft uses various physical security mechanisms in its cloud datacenters.

Identity and access
At this layer, it's important to:

- Control access to infrastructure and change control.
- Use single sign-on (SSO) and multifactor authentication.
- Audit events and changes.

The identity and access layer is all about ensuring that identities are secure, access is granted only to what's needed, and sign-in events and changes are logged.

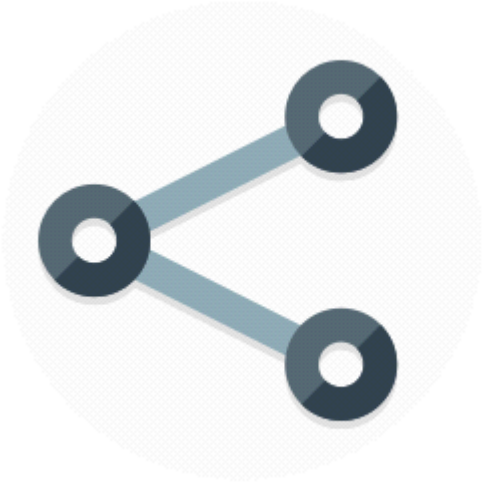


Perimeter

At this layer, it's important to:

- Use DDoS protection to filter large-scale attacks before they can affect the availability of a system for users.
- Use perimeter firewalls to identify and alert on malicious attacks against your network.

At the network perimeter, it's about protecting from network-based attacks against your resources. Identifying these attacks, eliminating their impact, and alerting you when they happen are important ways to keep your network secure.



Network

At this layer, it's important to:

- Limit communication between resources.
- Deny by default.
- Restrict inbound internet access and limit outbound access where appropriate.
- Implement secure connectivity to on-premises networks.

At this layer, the focus is on limiting the network connectivity across all your resources to allow only what's required. By limiting this communication, you reduce the risk of an attack spreading to other systems in your network.

Compute

At this layer, it's important to:

- Secure access to virtual machines.
- Implement endpoint protection on devices and keep systems patched and current.

Malware, unpatched systems, and improperly secured systems open your environment to attacks. The focus in this layer is on making sure that your compute resources are secure and that you have the proper controls in place to minimize security issues.

Application

At this layer, it's important to:

- Ensure that applications are secure and free of vulnerabilities.
- Store sensitive application secrets in a secure storage medium.
- Make security a design requirement for all application development.

Integrating security into the application development lifecycle helps reduce the number of vulnerabilities introduced in code. Every development team should ensure that its applications are secure by default.

Data
In almost all cases, attackers are after data:

- Stored in a database.
- Stored on disk inside virtual machines.
- Stored in software as a service (SaaS) applications, such as Office 365.
- Managed through cloud storage.

Those who store and control access to data are responsible for ensuring that it's properly secured. Often, regulatory requirements dictate the controls and processes that must be in place to ensure the confidentiality, integrity, and availability of the data.

Security posture

Your *security posture* is your organization's ability to protect from and respond to security threats. The common principles used to define a security posture are *confidentiality*, *integrity*, and *availability*, known collectively as CIA.

- Confidentiality
  The *principle of least privilege* means restricting access to information only to individuals explicitly granted access, at only the level that they need to perform their work. This information includes protection of user passwords, email content, and access levels to applications and underlying infrastructure.
- Integrity
  Prevent unauthorized changes to information:
- At rest: when it's stored.
- In transit: when it's being transferred from one place to another, including from a local computer to the cloud.
  A common approach used in data transmission is for the sender to create a unique fingerprint of the data by using a one-way hashing algorithm. The hash is sent to the receiver along with the data. The receiver recalculates the data's hash and compares it to the original to ensure that the data wasn't lost or modified in transit.
- Availability
  Ensure that services are functioning and can be accessed only by authorized users. *Denial-of-service attacks* are designed to degrade the availability of a system,

affecting its users.

From <https://docs.microsoft.com/en-us/learn/modules/secure-network-connectivity-azure/2-what-is-defense-in-depth>

Protect virtual networks by using Azure Firewall

- 3 minutes

A *firewall* is a network security device that monitors incoming and outgoing network traffic and decides whether to allow or block specific traffic based on a defined set of security rules. You can create firewall rules that specify ranges of IP addresses. Only clients granted IP addresses from within those ranges are allowed to access the destination server. Firewall rules can also include specific network protocol and port information.

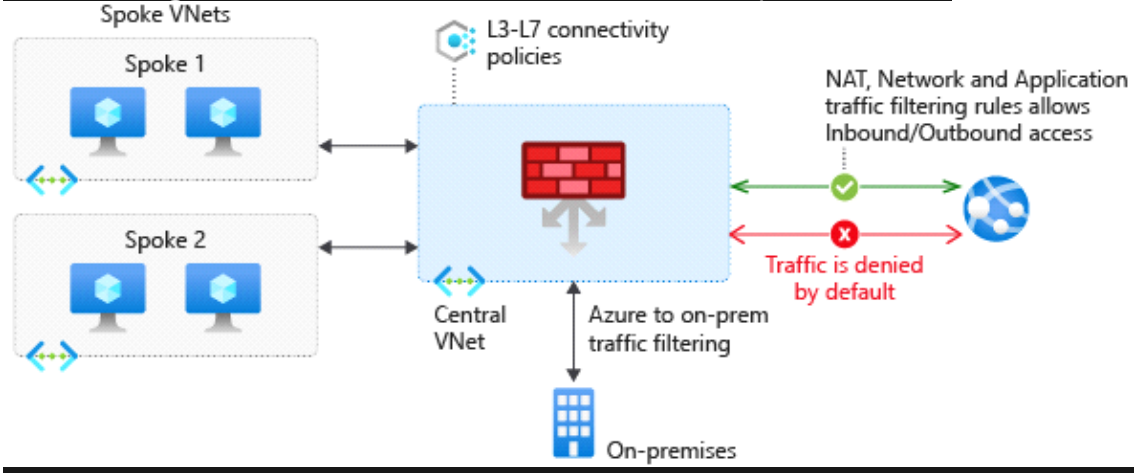
Tailwind Traders currently runs firewall appliances, which combine hardware and software, to protect its on-premises network. These firewall appliances require a monthly licensing fee to operate, and they require IT staff to perform routine maintenance. As Tailwind Traders moves to the cloud, the IT manager wants to know what Azure services can protect both the company's cloud networks and its on-premises networks.

In this part, you explore Azure Firewall.

What's Azure Firewall?

Azure Firewall is a managed, cloud-based network security service that helps protect resources in your Azure virtual networks. A virtual network is similar to a traditional network that you'd operate in your own datacenter. It's a fundamental building block for your private network that enables virtual machines and other compute resources to securely communicate with each other, the internet, and on-premises networks.

Here's a diagram that shows a basic Azure Firewall implementation:



Azure Firewall is a *stateful* firewall. A stateful firewall analyzes the complete context of a network connection, not just an individual packet of network traffic. Azure Firewall features high availability and unrestricted cloud scalability.

Azure Firewall provides a central location to create, enforce, and log application and

network connectivity policies across subscriptions and virtual networks. Azure Firewall uses a static (unchanging) public IP address for your virtual network resources, which enables outside firewalls to identify traffic coming from your virtual network. The service is integrated with Azure Monitor to enable logging and analytics.
Azure Firewall provides many features, including:

- Built-in high availability.
- Unrestricted cloud scalability.
- Inbound and outbound filtering rules.
- Inbound Destination Network Address Translation (DNAT) support.
- Azure Monitor logging.

You typically deploy Azure Firewall on a central virtual network to control general network access.

What can I configure with Azure Firewall?

With Azure Firewall, you can configure:

- Application rules that define fully qualified domain names (FQDNs) that can be accessed from a subnet.
- Network rules that define source address, protocol, destination port, and destination address.
- Network Address Translation (NAT) rules that define destination IP addresses and ports to translate inbound requests.

Azure Application Gateway also provides a firewall that's called the *web application firewall* (WAF). WAF provides centralized, inbound protection for your web applications against common exploits and vulnerabilities. Azure Front Door and Azure Content Delivery Network also provide WAF services.

From <https://docs.microsoft.com/en-us/learn/modules/secure-network-connectivity-azure/3-protect-network-azure-firewall>

Protect from DDoS attacks by using Azure DDoS Protection

- 3 minutes

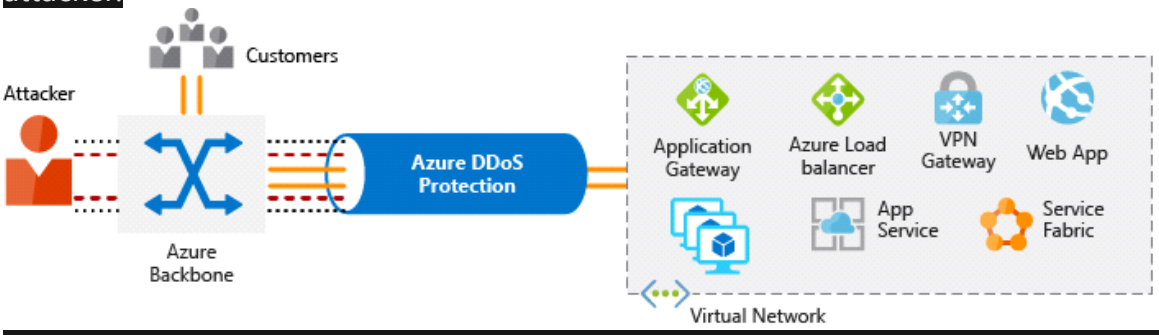
Any large company can be the target of a large-scale network attack. Tailwind Traders is no exception. Attackers might flood your network to make a statement or simply for the challenge. As Tailwind Traders moves to the cloud, it wants to understand how Azure can help prevent distributed denial of service (DDoS) and other attacks.
In this part, you learn how Azure DDoS Protection (Standard service tier) helps protect your Azure resources from DDoS attacks. First, let's define what a DDoS attack is.

What are DDoS attacks?

A distributed denial of service attack attempts to overwhelm and exhaust an application's resources, making the application slow or unresponsive to legitimate users. DDoS attacks can target any resource that's publicly reachable through the internet, including websites.

What is Azure DDoS Protection?

Azure DDoS Protection (Standard) helps protect your Azure resources from DDoS attacks.
When you combine DDoS Protection with recommended application design practices, you help provide a defense against DDoS attacks. DDoS Protection uses the scale and elasticity of Microsoft's global network to bring DDoS mitigation capacity to every Azure region. The DDoS Protection service helps protect your Azure applications by analyzing and discarding DDoS traffic at the Azure network edge, before it can affect your service's availability.
This diagram shows network traffic flowing into Azure from both customers and an attacker:



DDoS Protection identifies the attacker's attempt to overwhelm the network and blocks further traffic from them, ensuring that traffic never reaches Azure resources. Legitimate traffic from customers still flows into Azure without any interruption of service.
DDoS Protection can also help you manage your cloud consumption. When you run on-premises, you have a fixed number of compute resources. But in the cloud, elastic computing means that you can automatically scale out your deployment to meet demand. A cleverly designed DDoS attack can cause you to increase your resource allocation, which incurs unneeded expense. DDoS Protection Standard helps ensure that the network load you process reflects customer usage. You can also receive credit for any costs accrued for scaled-out resources during a DDoS attack.

What service tiers are available to DDoS Protection?

DDoS Protection provides these service tiers:

- Basic
  The Basic service tier is automatically enabled for free as part of your Azure subscription.
  Always-on traffic monitoring and real-time mitigation of common network-level attacks provide the same defenses that Microsoft's online services use. The Basic

service tier ensures that Azure infrastructure itself is not affected during a large-scale DDoS attack.
The Azure global network is used to distribute and mitigate attack traffic across Azure regions.

- Standard
  The Standard service tier provides additional mitigation capabilities that are tuned specifically to Azure Virtual Network resources. DDoS Protection Standard is relatively easy to enable and requires no changes to your applications.
  The Standard tier provides always-on traffic monitoring and real-time mitigation of common network-level attacks. It provides the same defenses that Microsoft's online services use.
  Protection policies are tuned through dedicated traffic monitoring and machine learning algorithms. Policies are applied to public IP addresses, which are associated with resources deployed in virtual networks such as Azure Load Balancer and Application Gateway.
  The Azure global network is used to distribute and mitigate attack traffic across Azure regions.

What kinds of attacks can DDoS Protection help prevent?

The Standard service tier can help prevent:

- Volumetric attacks
  The goal of this attack is to flood the network layer with a substantial amount of seemingly legitimate traffic.
- Protocol attacks
  These attacks render a target inaccessible by exploiting a weakness in the layer 3 and layer 4 protocol stack.
- Resource-layer (application-layer) attacks (only with web application firewall)
  These attacks target web application packets to disrupt the transmission of data between hosts. You need a web application firewall (WAF) to protect against L7 attacks. DDoS Protection Standard protects the WAF from volumetric and protocol attacks.

From <https://docs.microsoft.com/en-us/learn/modules/secure-network-connectivity-azure/4-protect-attacks-azure-ddos-protection>

Filter network traffic by using network security groups

- 2 minutes

Although Azure Firewall and Azure DDoS Protection can help control what traffic can come from outside sources, Tailwind Traders also wants to understand how to protect its internal networks on Azure. Doing so will give the company an extra layer of defense

against attacks.
In this part, you examine network security groups (NSGs).

What are network security groups?

A network security group enables you to filter network traffic to and from Azure resources within an Azure virtual network. You can think of NSGs like an internal firewall. An NSG can contain multiple inbound and outbound security rules that enable you to filter traffic to and from resources by source and destination IP address, port, and protocol.

How do I specify NSG rules?

A network security group can contain as many rules as you need, within Azure subscription limits. Each rule specifies these properties:

Property	Description
Name	A unique name for the NSG.
Priority	A number between 100 and 4096. Rules are processed in priority order, with lower numbers processed before higher numbers.
Source or Destination	A single IP address or IP address range, service tag, or application security group.
Protocol	TCP, UDP, or Any.
Direction	Whether the rule applies to inbound or outbound traffic.
Port Range	A single port or range of ports.
Action	Allow or Deny.

HOW DO I SPECIFY NSG RULES?

When you create a network security group, Azure creates a series of default rules to provide a baseline level of security. You can't remove the default rules, but you can override them by creating new rules with higher priorities.

From <https://docs.microsoft.com/en-us/learn/modules/secure-network-connectivity-azure/5-filter-traffic-network-security-groups>

Exercise - Configure network access to a VM by using a network security group

- 10 minutes

This module requires a sandbox to complete. A sandbox gives you access to free resources. Your personal subscription will not be charged. The sandbox may only be used to complete training on Microsoft Learn. Use for any other reason is prohibited, and may result in permanent loss of access to the sandbox.

Sign in to activate sandbox

In this exercise, you configure network access to a virtual machine (VM) running on Azure.
You start by creating a Linux VM and installing Nginx, a popular web server, on that VM. To make your web server accessible, you then create a network security group (NSG) rule that allows inbound access on port 80 (HTTP).
There are many ways to create and manage VMs, including their network settings. For example, you can use the Azure portal, the Azure CLI, Azure PowerShell, or an Azure Resource Manager (ARM) template.
Here, you use the Azure CLI. The Azure CLI enables you to connect to Azure and run administrative commands on Azure resources. As with other command-line interfaces, you can run commands directly from a terminal or you can add commands to a Bash script or a PowerShell script. The Azure CLI runs on Windows, macOS, or Linux.
Here, you access the Azure CLI from Azure Cloud Shell. Cloud Shell is a browser-based shell experience that you use to manage and develop Azure resources. Think of Cloud Shell as an interactive console that runs in the cloud.
If you're new to the Azure CLI or to Cloud Shell, just follow along.

Create a Linux virtual machine and install Nginx

Use the following Azure CLI commands to create a Linux VM and install Nginx. After your VM is created, you'll use the Custom Script Extension to install Nginx. The Custom Script Extension is an easy way to download and run scripts on your Azure VMs. It's just one of the many ways you can configure the system after your VM is up and running.

1. From Cloud Shell, run the following `az vm create` command to create a Linux VM:
   Azure CLICopy
   ```
   az vm create \
     --resource-group [sandbox resource group name] \
     --name my-vm \
     --image UbuntuLTS \
     --admin-username azureuser \
     --generate-ssh-keys
   ```
   Your VM will take a few moments to come up.
   You name the VM my-vm. You use this name to refer to the VM in later steps.
2. Run the following `az vm extension set` command to configure Nginx on your VM:
   Azure CLICopy
   ```
   az vm extension set \
     --resource-group [sandbox resource group name] \
     --vm-name my-vm \
     --name customScript \
     --publisher Microsoft.Azure.Extensions \
     --version 2.1 \
     --settings '{"fileUris":["https://raw.githubusercontent.com/MicrosoftDocs/mslearn-welcome-to-azure/master/configure-nginx.sh"]}' \
     --protected-settings '{"commandToExecute": "./configure-nginx.sh"}'
   ```
   This command uses the Custom Script Extension to run a Bash script on your VM.

The script is stored on GitHub.
While the command runs, you can choose to examine the Bash script from a separate browser tab.
To summarize, the script:

3. Runs apt-get update to download the latest package information from the internet. This step helps ensure that the next command can locate the latest version of the Nginx package.
4. Installs Nginx.
5. Sets the home page, */var/www/html/index.html*, to print a welcome message that includes your VM's host name.

Access your web server

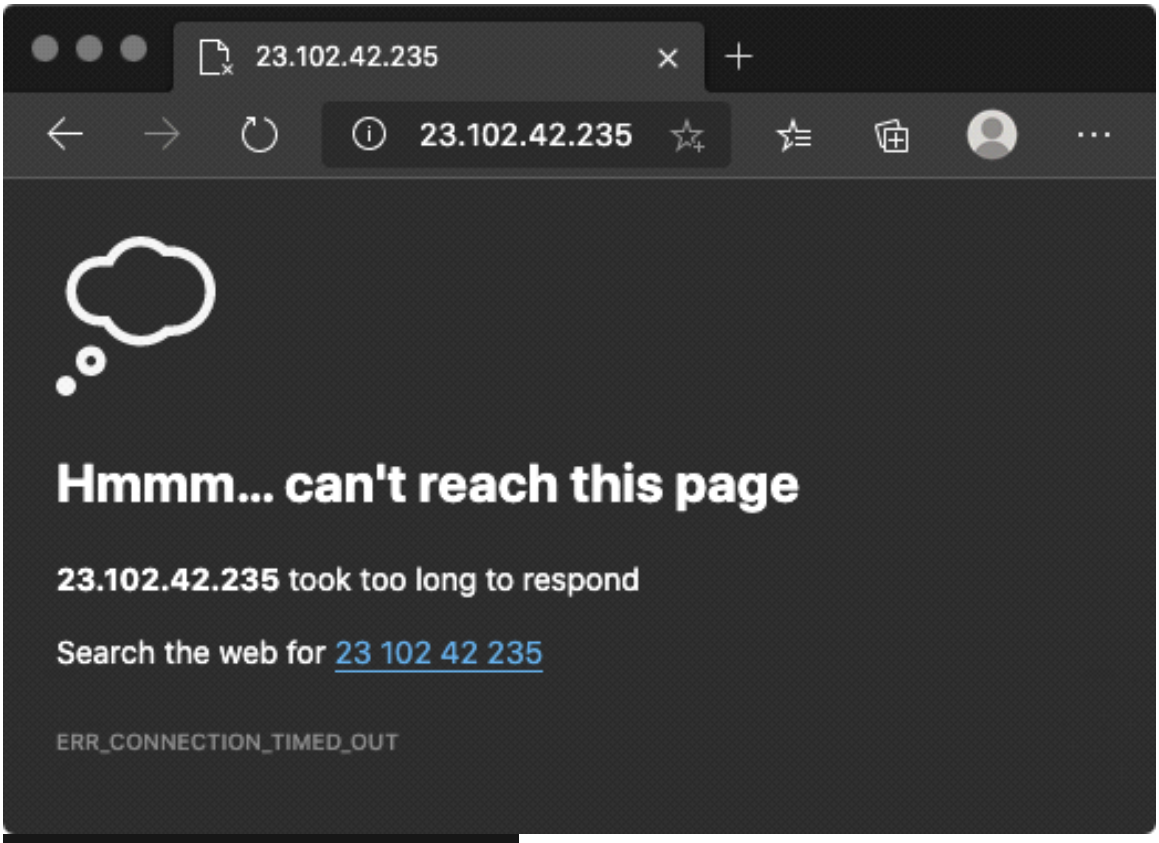
In this procedure, you get the IP address for your VM and attempt to access your web server's home page.

1. Run the following az vm list-ip-addresses command to get your VM's IP address and store the result as a Bash variable:
   Azure CLICopy
   ```
   IPADDRESS="$(az vm list-ip-addresses \
     --resource-group [sandbox resource group name] \
     --name my-vm \
     --query "[].virtualMachine.network.publicIpAddresses[*].ipAddress" \
     --output tsv)"
   ```
2. Run the following curl command to download the home page:
   BashCopy
   ```
   curl --connect-timeout 5 http://$IPADDRESS
   ```

   The --connect-timeout argument specifies to allow up to five seconds for the connection to occur.
   After five seconds, you see an error message that states that the connection timed out:
   OutputCopy
   ```
   curl: (28) Connection timed out after 5001 milliseconds
   ```

   This message means that the VM was not accessible within the timeout period.
3. As an optional step, try to access the web server from a browser:
4. Run the following to print your VM's IP address to the console:
   BashCopy
   ```
   echo $IPADDRESS
   ```

   You see an IP address, for example, *23.102.42.235*.
5. Copy the IP address that you see to the clipboard.
6. Open a new browser tab and go to your web server.
   After a few moments, you see that the connection isn't happening. If you wait for the browser to time out, you'll see something like this:



Keep this browser tab open for later.

List the current network security group rules

Your web server wasn't accessible. To find out why, let's examine your current NSG rules.

1. Run the following `az network nsg list` command to list the network security groups that are associated with your VM:

   Azure CLICopy

   ```
   az network nsg list \
     --resource-group [sandbox resource group name] \
     --query '[].name' \
     --output tsv
   ```

   You see this:

   OutputCopy

   ```
   my-vmNSG
   ```

   Every VM on Azure is associated with at least one network security group. In this case, Azure created an NSG for you called *my-vmNSG*.

2. Run the following `az network nsg rule list` command to list the rules associated with the NSG named *my-vmNSG*:

   Azure CLICopy

   ```
   az network nsg rule list \
     --resource-group [sandbox resource group name] \
     --nsg-name my-vmNSG
   ```

You see a large block of text in JSON format in the output. In the next step, you'll run a similar command that makes this output easier to read.

3. Run the `az network nsg rule list` command a second time.
   This time, use the `--query` argument to retrieve only the name, priority, affected ports, and access (Allow or Deny) for each rule.
   The `--output` argument formats the output as a table so that it's easy to read.
   Azure CLICopy
   ```
   az network nsg rule list \
     --resource-group [sandbox resource group name] \
     --nsg-name my-vmNSG \
     --query '[].{Name:name, Priority:priority, Port:destinationPortRange, Access:access}' \
     --output table
   ```

   You see this:
   OutputCopy
   ```
   Name              Priority    Port    Access
   ----------------  ----------  ------  --------
   default-allow-ssh  1000        22      Allow
   ```

   You see the default rule, *default-allow-ssh*. This rule allows inbound connections over port 22 (SSH). SSH (Secure Shell) is a protocol that's used on Linux to allow administrators to access the system remotely.
   The priority of this rule is 1000. Rules are processed in priority order, with lower numbers processed before higher numbers.

By default, a Linux VM's NSG allows network access only on port 22. This enables administrators to access the system. You need to also allow inbound connections on port 80, which allows access over HTTP.

Create the network security rule

Here, you create a network security rule that allows inbound access on port 80 (HTTP).

1. Run the following `az network nsg rule create` command to create a rule called *allow-http* that allows inbound access on port 80:
   Azure CLICopy
   ```
   az network nsg rule create \
     --resource-group [sandbox resource group name] \
     --nsg-name my-vmNSG \
     --name allow-http \
     --protocol tcp \
     --priority 100 \
     --destination-port-range 80 \
     --access Allow
   ```

   For learning purposes, here you set the priority to 100. In this case, the priority doesn't matter. You would need to consider the priority if you had overlapping port ranges.
2. To verify the configuration, run `az network nsg rule list` to see the updated list of rules:

Azure CLICopy

```
az network nsg rule list \
  --resource-group [sandbox resource group name] \
  --nsg-name my-vmNSG \
  --query '[].{Name:name, Priority:priority, Port:destinationPortRange, Access:access}' \
  --output table
```

You see this both the *default-allow-ssh* rule and your new rule, *allow-http*:

OutputCopy

```
Name              Priority    Port    Access
----------------- ----------  ------  --------
default-allow-ssh  1000       22      Allow
allow-http         100        80      Allow
```

Access your web server again

Now that you've configured network access to port 80, let's try to access the web server a second time.

1. Run the same curl command that you ran earlier:

   BashCopy

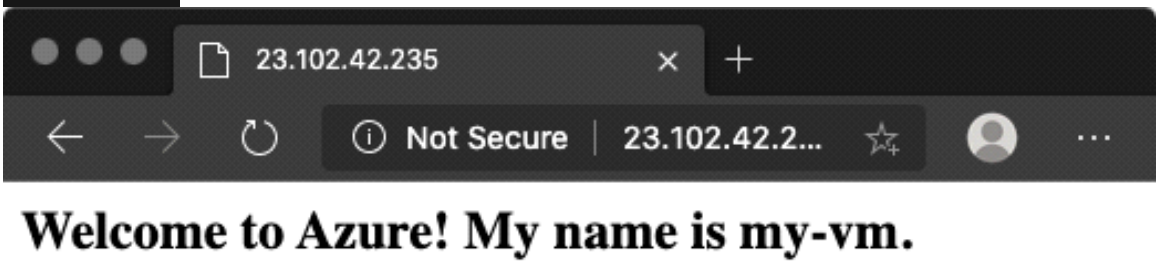
   ```
   curl --connect-timeout 5 http://$IPADDRESS
   ```

   You see this:

   HTMLCopy

   ```
   <html><body><h2>Welcome to Azure! My name is my-vm.</h2></body></html>
   ```

2. As an optional step, refresh your browser tab that points to your web server. You see this:



Welcome to Azure! My name is my-vm.

Clean up

The sandbox automatically cleans up your resources when you're finished with this module.
When you're working in your own subscription, it's a good idea at the end of a project to identify whether you still need the resources you created. Resources left running can cost you money. You can delete resources individually or delete the resource group to delete the entire set of resources.
Nice work. In practice, you can create a standalone network security group that includes the inbound and outbound network access rules you need. If you have multiple VMs that serve the same purpose, you can assign that NSG to each VM at the time you create it. This technique enables you to control network access to multiple VMs under a single, central set of rules.

Next unit: Combine Azure services to create a complete network security solution

Continue

From <https://docs.microsoft.com/en-us/learn/modules/secure-network-connectivity-azure/6-configure-access-network-security-group>

Combine Azure services to create a complete network security solution

- 3 minutes

When you're considering an Azure security solution, consider all the elements of defense in depth.
Here are some recommendations on how to combine Azure services to create a complete network security solution.

Secure the perimeter layer

The perimeter layer is about protecting your organization's resources from network-based attacks. Identifying these attacks, alerting the appropriate security teams, and eliminating their impact are important to keeping your network secure. To do this:

- Use Azure DDoS Protection to filter large-scale attacks before they can cause a denial of service for users.
- Use perimeter firewalls with Azure Firewall to identify and alert on malicious attacks against your network.

Secure the network layer

At this layer, the focus is on limiting network connectivity across all of your resources to allow only what's required. Segment your resources and use network-level controls to restrict communication to only what's needed.
By restricting connectivity, you reduce the risk of lateral movement throughout your network from an attack. Use network security groups to create rules that define allowed inbound and outbound communication at this layer. Here are some recommended practices:

- Limit communication between resources by segmenting your network and configuring access controls.
- Deny by default.
- Restrict inbound internet access and limit outbound where appropriate.
- Implement secure connectivity to on-premises networks.

Combine services

You can combine Azure networking and security services to manage your network security and provide increased layered protection. Here are two ways you can combine services:

- Network security groups and Azure Firewall
  Azure Firewall complements the functionality of network security groups. Together, they provide better defense-in-depth network security.
  Network security groups provide distributed network-layer traffic filtering to limit traffic to resources within virtual networks in each subscription.
  Azure Firewall is a fully stateful, centralized network firewall as a service. It provides network-level and application-level protection across different subscriptions and virtual networks.
- Azure Application Gateway web application firewall and Azure Firewall
  Web application firewall (WAF) is a feature of Azure Application Gateway that provides your web applications with centralized, inbound protection against common exploits and vulnerabilities.
  Azure Firewall provides:
- Inbound protection for non-HTTP/S protocols (for example, RDP, SSH, and FTP).
- Outbound network-level protection for all ports and protocols.
- Application-level protection for outbound HTTP/S.
  Combining them provides more layers of protection.

From <https://docs.microsoft.com/en-us/learn/modules/secure-network-connectivity-azure/7-combine-services-complete-solution>

Part 5: Describe identity, governance, privacy, and compliance features

Thursday, January 28, 2021 10:50 AM

Secure access to your applications by using Azure identity services

Thursday, January 28, 2021 10:50 AM

Learn how Azure Active Directory helps you manage and secure identities. Also see how single sign-on, multifactor authentication, and Conditional Access enable your users to securely access resources and applications from your intranet and from public networks.
Overview

- Introduction 1 min
- Compare authentication and authorization 2 min
- What is Azure Active Directory? 5 min
- What are multifactor authentication and Conditional Access? 4 min
- Knowledge check 3 min
- Summary 2 min

From <https://docs.microsoft.com/en-us/learn/paths/az-900-describe-identity-governance-privacy-compliance-features/>

Introduction

- 1 minute

Traditionally, protecting access to systems and data involved the on-premises network perimeter and physical access controls.
With people increasingly able to work from anywhere, plus the rise of bring your own device (BYOD) strategies, mobile applications, and cloud applications, many of those access points are now outside the company's physical networks.
Identity has become the new primary security boundary. Accurately proving that someone is a valid user of your system, with an appropriate level of access, is critical to maintaining control of your data. This identity layer is now more often the target of attack than the network is.

Meet Tailwind Traders

Tailwind Traders is a fictitious home improvement retailer. It operates retail hardware stores across the globe and online.

Tailwind Traders specializes in competitive pricing, fast shipping, and a large range of items. It's looking at cloud technologies to improve business operations and support

growth into new markets. By moving to the cloud, the company plans to enhance its shopping experience to further differentiate itself from competitors.

How will Tailwind Traders secure access to its cloud applications?

The mobile workforce of Tailwind Traders is increasing, as are the number of applications that the company runs in the cloud.
Retail employees located around the world are issued tablet devices from which they can create orders for customers, track delivery schedules, and plan their work schedules.
Delivery drivers can use their own mobile devices to access scheduling and logistics applications. Some delivery drivers are permanent employees of Tailwind Traders.
Others work on short-term contract.
Tailwind Traders uses Active Directory to secure its on-premises environment. It needs to ensure that only employees can sign in and access the company's business applications. It also needs to ensure that short-term staff can access these applications only when they're under active contract.
How can Azure Active Directory (Azure AD) help Tailwind Traders consistently secure all of its applications accessed from the intranet and from public networks?

Learning objectives

After completing this module, you'll be able to:

- Explain the difference between authentication and authorization.
- Describe how Azure AD provides identity and access management.
- Explain the role that single sign-on (SSO), multifactor authentication, and Conditional Access play in managing user identity.

Prerequisites

- You should be familiar with basic computing concepts and terminology.
- Familiarity with cloud computing is helpful but isn't necessary.

From <https://docs.microsoft.com/en-us/learn/modules/secure-access-azure-identity-services/1-introduction>

Compare authentication and authorization

- 2 minutes

Recall that Tailwind Traders must ensure that only employees can sign in and access its business applications.
Tailwind Traders also needs to ensure that employees can access only authorized applications. For example, all employees can access inventory and pricing software, but only store managers can access payroll and certain accounting software.
Two fundamental concepts that you need to understand when talking about identity

and access are *authentication* (AuthN) and *authorization* (AuthZ). Authentication and authorization both support everything else that happens. They occur sequentially in the identity and access process.
Let's take a brief look at each.

What is authentication?

Authentication is the process of establishing the identity of a person or service that wants to access a resource. It involves the act of challenging a party for legitimate credentials and provides the basis for creating a security principal for identity and access control. It establishes whether the user is who they say they are.

What is authorization?

Authentication establishes the user's identity, but authorization is the process of establishing what level of access an authenticated person or service has. It specifies what data they're allowed to access and what they can do with it.

How are authentication and authorization related?

Here's a diagram that shows the relationship between authentication and authorization:

The identification card represents credentials that the user has to prove their identity (you'll learn more about the types of credentials later in this module.) Once authenticated, authorization defines what kinds of applications, resources, and data that user can access.

From <https://docs.microsoft.com/en-us/learn/modules/secure-access-azure-identity-services/2-compare-authentication-authorization>

What is Azure Active Directory?

- 5 minutes

In this part, you learn how Azure Active Directory (Azure AD) provides identity services that enable your users to sign in and access both Microsoft cloud applications and cloud

applications that you develop. You also learn how Azure AD supports single sign-on (SSO).

Tailwind Traders already uses Active Directory to secure its on-premises environments. The company doesn't want its users to have a different username and password to remember for accessing applications and data in the cloud. Can the company integrate its existing Active Directory instance with cloud identity services to create a seamless experience for its users?

Let's start with how Azure AD compares to Active Directory.

How does Azure AD compare to Active Directory?

Active Directory is related to Azure AD, but they have some key differences.

Microsoft introduced Active Directory in Windows 2000 to give organizations the ability to manage multiple on-premises infrastructure components and systems by using a single identity per user.

For on-premises environments, Active Directory running on Windows Server provides an identity and access management service that's managed by your own organization.

Azure AD is Microsoft's cloud-based identity and access management service. With Azure AD, you control the identity accounts, but Microsoft ensures that the service is available globally. If you've worked with Active Directory, Azure AD will be familiar to you.

When you secure identities on-premises with Active Directory, Microsoft doesn't monitor sign-in attempts. When you connect Active Directory with Azure AD, Microsoft can help protect you by detecting suspicious sign-in attempts at no extra cost. For example, Azure AD can detect sign-in attempts from unexpected locations or unknown devices.

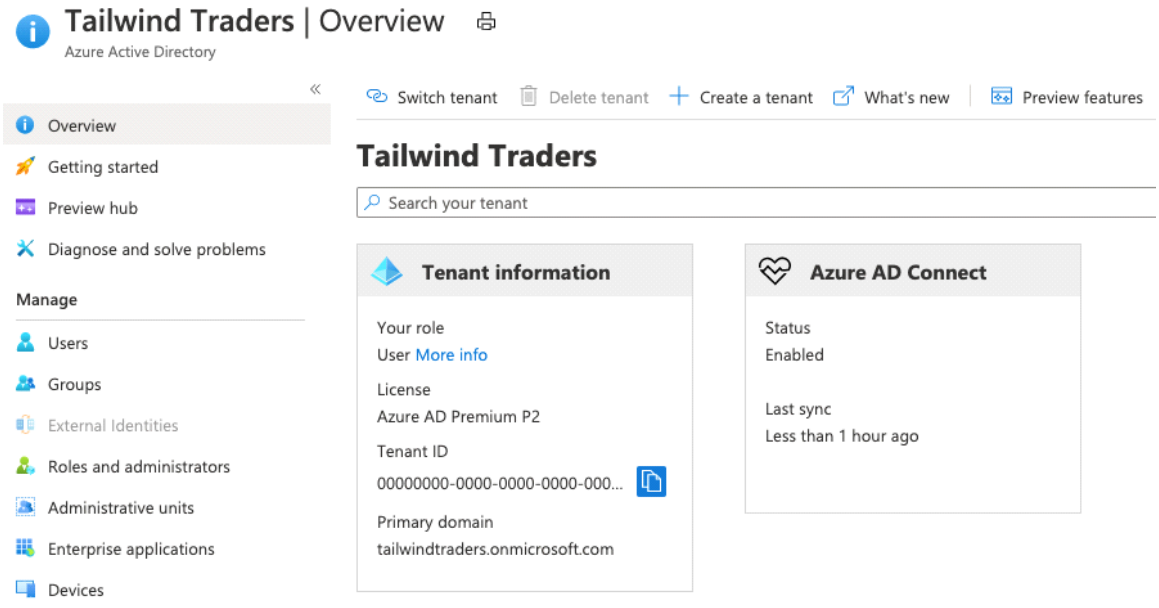
Who uses Azure AD?

Azure AD is for:

- IT administrators
  Administrators can use Azure AD to control access to applications and resources based on their business requirements.
- App developers
  Developers can use Azure AD to provide a standards-based approach for adding functionality to applications that they build, such as adding SSO functionality to an app or enabling an app to work with a user's existing credentials.
- Users
  Users can manage their identities. For example, self-service password reset enables users to change or reset their password with no involvement from an IT administrator or help desk.
- Online service subscribers
  Microsoft 365, Microsoft Office 365, Azure, and Microsoft Dynamics CRM Online subscribers are already using Azure AD.

A *tenant* is a representation of an organization. A tenant is typically separated from other tenants and has its own identity.
Each Microsoft 365, Office 365, Azure, and Dynamics CRM Online tenant is automatically an Azure AD tenant.

Here's a screenshot of what an IT administrator might see in the Azure portal when working with Active Directory:



What services does Azure AD provide?

Azure AD provides services such as:

- Authentication
  This includes verifying identity to access applications and resources. It also includes providing functionality such as self-service password reset, multifactor authentication, a custom list of banned passwords, and smart lockout services.
- Single sign-on
  SSO enables you to remember only one username and one password to access multiple applications. A single identity is tied to a user, which simplifies the security model. As users change roles or leave an organization, access modifications are tied to that identity, which greatly reduces the effort needed to change or disable accounts.
- Application management
  You can manage your cloud and on-premises apps by using Azure AD. Features like Application Proxy, SaaS apps, the My Apps portal (also called the *access panel*), and single-sign on provide a better user experience.
- Device management
  Along with accounts for individual people, Azure AD supports the registration of devices. Registration enables devices to be managed through tools like Microsoft Intune. It also allows for device-based conditional access policies to restrict access attempts to only those coming from known devices, regardless of the requesting user account.

What kinds of resources can Azure AD help secure?

Azure AD helps users access both external and internal resources.
External resources might include Microsoft Office 365, the Azure portal, and thousands of other software as a service (SaaS) applications.
Internal resources might include apps on your corporate network and intranet, along with any cloud applications developed within your organization.

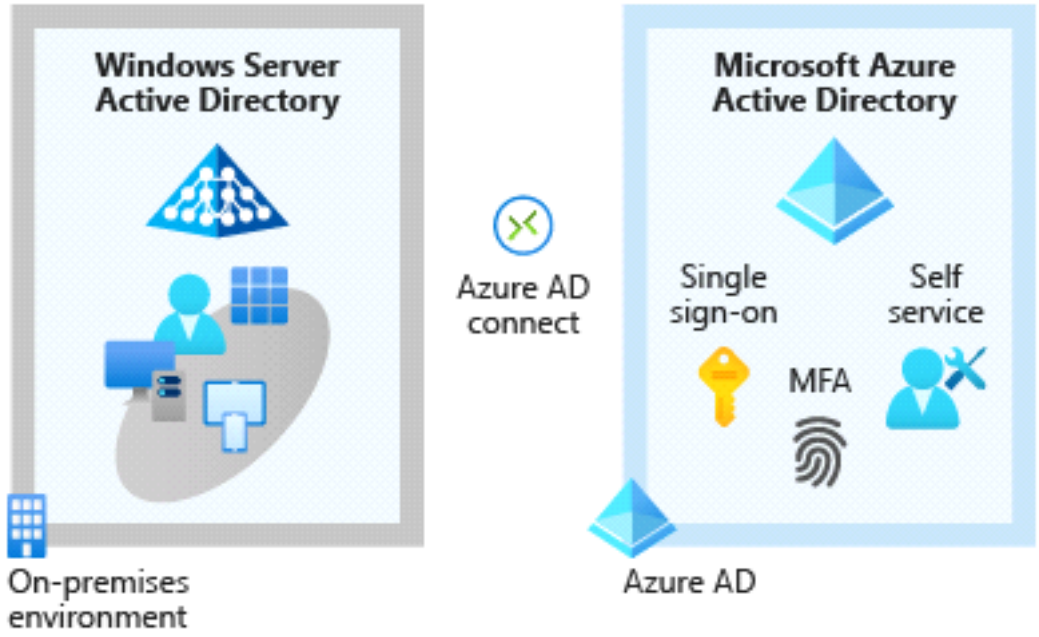
What's single sign-on?

Single sign-on enables a user to sign in one time and use that credential to access multiple resources and applications from different providers.
More identities mean more passwords to remember and change. Password policies can vary among applications. As complexity requirements increase, it becomes increasingly difficult for users to remember them. The more passwords a user has to manage, the greater the risk of a credential-related security incident.
Consider the process of managing all those identities. Additional strain is placed on help desks as they deal with account lockouts and password reset requests. If a user leaves an organization, tracking down all those identities and ensuring they are disabled can be challenging. If an identity is overlooked, this might allow access when it should have been eliminated.
With SSO, you need to remember only one ID and one password. Access across applications is granted to a single identity that's tied to the user, which simplifies the security model. As users change roles or leave an organization, access is tied to a single identity. This change greatly reduces the effort needed to change or disable accounts.
Using SSO for accounts makes it easier for users to manage their identities and increases your security capabilities.
You'll find resources at the end of this module about how to enable SSO through Azure AD.

How can I connect Active Directory with Azure AD?

Connecting Active Directory with Azure AD enables you to provide a consistent identity experience to your users.
There are a few ways to connect your existing Active Directory installation with Azure AD. Perhaps the most popular method is to use Azure AD Connect.
Azure AD Connect synchronizes user identities between on-premises Active Directory and Azure AD. Azure AD Connect synchronizes changes between both identity systems, so you can use features like SSO, multifactor authentication, and self-service password reset under both systems. Self-service password reset prevents users from using known compromised passwords.
Here's a diagram that shows how Azure AD Connect fits between on-premises Active

Directory and Azure AD:



As Tailwind Traders integrates its existing Active Directory instance with Azure AD, it creates a consistent access model across its organization. Doing so greatly simplifies its ability to sign in to different applications, manage changes to user identities and control, and monitor and block unusual access attempts.

From <https://docs.microsoft.com/en-us/learn/modules/secure-access-azure-identity-services/3-what-is-azure-active-directory>

What are multifactor authentication and Conditional Access?

- 4 minutes

Tailwind Traders allows delivery drivers to use their own mobile devices to access scheduling and logistics applications. Some delivery drivers are permanent employees of Tailwind Traders. Others work on short-term contract. How can the IT department ensure that an access attempt is really from a valid Tailwind Traders worker?

In this part, you'll learn about two processes that enable secure authentication: Azure AD Multi-Factor Authentication and Conditional Access. Let's start with a brief look at what multifactor authentication is in general.

What's multifactor authentication?

Multifactor authentication is a process where a user is prompted during the sign-in process for an additional form of identification. Examples include a code on their mobile phone or a fingerprint scan.

Think about how you sign in to websites, email, or online gaming services. In addition to your username and password, have you ever needed to enter a code that was sent to

your phone? If so, you've used multifactor authentication to sign in.
Multifactor authentication provides additional security for your identities by requiring two or more elements to fully authenticate.
These elements fall into three categories:

- Something the user knows
  This might be an email address and password.
- Something the user has
  This might be a code that's sent to the user's mobile phone.
- Something the user is
  This is typically some sort of biometric property, such as a fingerprint or face scan that's used on many mobile devices.

Multifactor authentication increases identity security by limiting the impact of credential exposure (for example, stolen usernames and passwords). With multifactor authentication enabled, an attacker who has a user's password would also need to have possession of their phone or their fingerprint to fully authenticate.
Compare multifactor authentication with single-factor authentication. Under single-factor authentication, an attacker would need only a username and password to authenticate. Multifactor authentication should be enabled wherever possible because it adds enormous benefits to security.

What's Azure AD Multi-Factor Authentication?

Azure AD Multi-Factor Authentication is a Microsoft service that provides multifactor authentication capabilities. Azure AD Multi-Factor Authentication enables users to choose an additional form of authentication during sign-in, such as a phone call or mobile app notification.
These services provide Azure AD Multi-Factor Authentication capabilities:

- Azure Active Directory
  The Azure Active Directory free edition enables Azure AD Multi-Factor Authentication for administrators with the *global admin* level of access, via the Microsoft Authenticator app, phone call, or SMS code. You can also enforce Azure AD Multi-Factor Authentication for all users via the Microsoft Authenticator app only, by enabling *security defaults* in your Azure AD tenant.
  Azure Active Directory Premium (P1 or P2 licenses) allows for comprehensive and granular configuration of Azure AD Multi-Factor Authentication through Conditional Access policies (explained shortly).
- Multifactor authentication for Office 365

- A subset of Azure AD Multi-Factor Authentication capabilities is part of your Office 365 subscription.

For more information on licenses and Azure AD Multi-Factor Authentication capabilities, see Available versions of Azure AD Multi-Factor Authentication .

What's Conditional Access?

Conditional Access is a tool that Azure Active Directory uses to allow (or deny) access to resources based on identity *signals*. These signals include who the user is, where the user is, and what device the user is requesting access from.

Conditional Access helps IT administrators:

- Empower users to be productive wherever and whenever.
- Protect the organization's assets.

Conditional Access also provides a more granular multifactor authentication experience for users. For example, a user might not be challenged for second authentication factor if they're at a known location. However, they might be challenged for a second authentication factor if their sign-in signals are unusual or they're at an unexpected location.

During sign-in, Conditional Access collects signals from the user, makes decisions based on those signals, and then enforces that decision by allowing or denying the access request or challenging for a multifactor authentication response.

Here's a diagram that illustrates this flow:

Here, the signal might be the user's location, the user's device, or the application that the user is trying to access.

Based on these signals, the decision might be to allow full access if the user is signing in from their usual location. If the user is signing in from an unusual location or a location that's marked as high risk, then access might be blocked entirely or possibly granted after the user provides a second form of authentication.

Enforcement is the action that carries out the decision. For example, the action is to allow access or require the user to provide a second form of authentication.

When can I use Conditional Access?

Conditional Access is useful when you need to:

- Require multifactor authentication to access an application.
  You can configure whether all users require multifactor authentication or only

certain users, such as administrators.
You can also configure whether multifactor authentication applies to access from all networks or only untrusted networks.

- Require access to services only through approved client applications.
  For example, you might want to allow users to access Office 365 services from a mobile device as long as they use approved client apps, like the Outlook mobile app.
- Require users to access your application only from managed devices.
  A *managed device* is a device that meets your standards for security and compliance.
- Block access from untrusted sources, such as access from unknown or unexpected locations.

Conditional Access comes with a *What If* tool, which helps you plan and troubleshoot your Conditional Access policies. You can use this tool to model your proposed Conditional Access policies across recent sign-in attempts from your users to see what the impact would have been if those policies had been enabled. The What If tool enables you to test your proposed Conditional Access policies before you implement them.

Where is Conditional Access available?

To use Conditional Access, you need an Azure AD Premium P1 or P2 license. If you have a Microsoft 365 Business Premium license, you also have access to Conditional Access features.

From <https://docs.microsoft.com/en-us/learn/modules/secure-access-azure-identity-services/4-what-are-mfa-conditional-access>

Build a cloud governance strategy on Azure

Thursday, January 28, 2021 10:52 AM

Learn how access policies, resource locks, and tags, as well as Azure services such as Azure Policy and Azure Blueprints, can help you build a comprehensive cloud governance strategy.

Overview

- Introduction 2 min
- Accelerate your cloud adoption journey by using the Cloud Adoption Framework for Azure 3 min
- Create a subscription governance strategy 3 min
- Control access to cloud resources by using Azure role-based access control 4 min
- Prevent accidental changes by using resource locks 3 min
- Exercise - Protect a storage account from accidental deletion by using a resource lock 8 min
- Organize your Azure resources by using tags 3 min
- Control and audit your resources by using Azure Policy 5 min
- Exercise - Restrict deployments to a specific location by using Azure Policy 8 min
- Govern multiple subscriptions by using Azure Blueprints 4 min
- Knowledge check 3 min
- Summary 2 min

From <https://docs.microsoft.com/en-us/learn/paths/az-900-describe-identity-governance-privacy-compliance-features/>

Introduction

- 2 minutes

The term *governance* describes the general process of establishing rules and policies and ensuring that those rules and policies are enforced.

When running in the cloud, a good governance strategy helps you maintain control over the applications and resources that you manage in the cloud. Maintaining control over your environment ensures that you stay compliant with:

- Industry standards, like PCI DSS .
- Corporate or organizational standards, such as ensuring that network data is encrypted.

Governance is most beneficial when you have:

- Multiple engineering teams working in Azure.
- Multiple subscriptions to manage.
- Regulatory requirements that must be enforced.
- Standards that must be followed for all cloud resources.

Meet Tailwind Traders

Tailwind Traders is a fictitious home improvement retailer. It operates retail hardware stores across the globe and online.

Tailwind Traders specializes in competitive pricing, fast shipping, and a large range of items. It's looking at cloud technologies to improve business operations and support growth into new markets. By moving to the cloud, the company plans to enhance its shopping experience to further differentiate itself from competitors.

How will Tailwind Traders improve agility while maintaining control?

Tailwind Traders is continuing its migration to the cloud. For its existing datacenter, development and test teams must submit support tickets to request access to virtual machines, storage, and networking components. It can take IT staff anywhere from two weeks to two months to purchase, provision, and configure these components.
By working in the cloud, you essentially have immediate access to compute, storage, and networking components. Many kinds of groups and users, including people from development, test, operations, and security teams, can potentially have direct access to cloud resources.
Going forward, Tailwind Traders could enforce similar processes that prevent teams from directly creating or configuring resources on Azure, similar to its existing approach where central IT provisions infrastructure. But the company knows that these restrictions reduce team agility and the ability to innovate. How can they enable innovation while still maintaining control?
In this module, you'll help the company explore ways it can enforce standards while still enabling teams to create and manage the cloud resources they need.

Learning objectives

After completing this module, you'll be able to:

- Make organizational decisions about your cloud environment by using the Cloud Adoption Framework for Azure.
- Define who can access cloud resources by using Azure role-based access control.
- Apply a resource lock to prevent accidental deletion of your Azure resources.
- Apply tags to your Azure resources to help describe their purpose.
- Control and audit how your resources are created by using Azure Policy.
- Enable governance at scale across multiple Azure subscriptions by using Azure Blueprints.

From <https://docs.microsoft.com/en-us/learn/modules/build-cloud-governance-strategy-azure/1-introduction>

Accelerate your cloud adoption journey by using the Cloud Adoption Framework for Azure

- 3 minutes

The Cloud Adoption Framework for Azure provides you with proven guidance to help with your cloud adoption journey. The Cloud Adoption Framework helps you create and implement the business and technology strategies needed to succeed in the cloud.

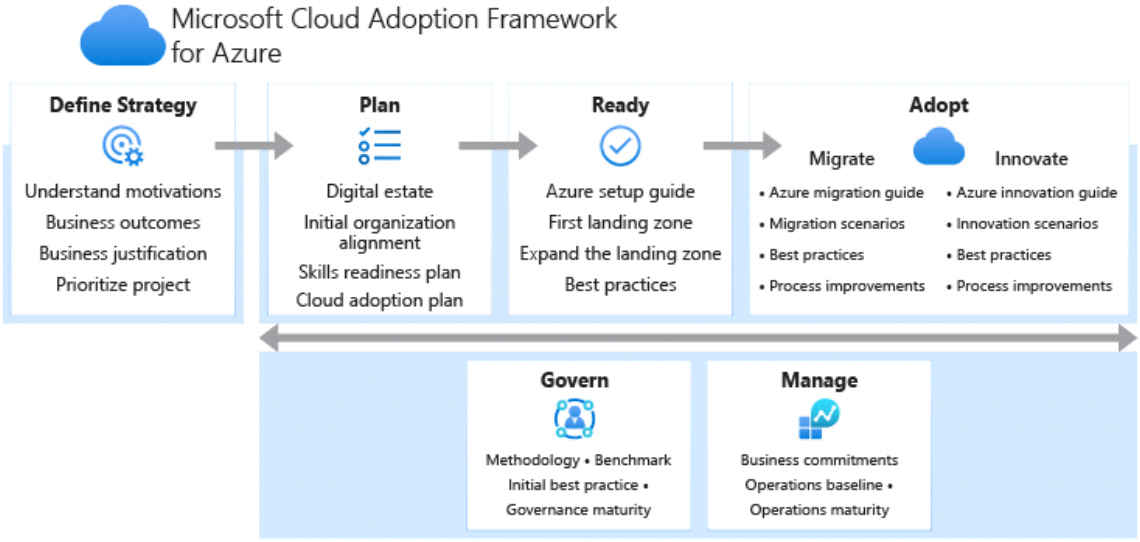
Tailwind Traders needs to control its cloud environment so that it complies with several industry standards, but it's not sure where to start. It has existing business requirements, and it understands how these requirements relate to its on-premises workloads. These requirements also must be met by any workloads it runs in the cloud.

You've been tasked with investigating what's available on Azure and to define and implement the governance strategy for Tailwind Traders. You decide to start with the Cloud Adoption Framework.

What's in the Cloud Adoption Framework?

The Cloud Adoption Framework consists of tools, documentation, and proven practices. The Cloud Adoption Framework includes these stages:

1. Define your strategy.
2. Make a plan.
3. Ready your organization.
4. Adopt the cloud.
5. Govern and manage your cloud environments.



The govern stage focuses on cloud governance. You can refer back to the Cloud Adoption Framework for recommended guidance as you build your cloud governance strategy.

To help build your adoption strategy, the Cloud Adoption Framework breaks out each stage into further exercises and steps. Let's take a brief look at each stage.

Define your strategy

Here, you answer why you're moving to the cloud and what you want to get out of cloud migration. Do you need to scale to meet demand or reach new markets? Will it reduce costs or increase business agility?
Here are the steps in this stage.

	Define and document your motivations: Meeting with stakeholders and leadership can help you answer why you're moving to the cloud.
	Document business outcomes: Meet with leadership from your finance, marketing, sales, and human resource groups to help you document your goals.
	Develop a business case: Validate that moving to the cloud gives you the right return on investment (ROI) for your efforts.
	Choose the right first project: Choose a project that's achievable but also shows progress toward your cloud migration goals.

DEFINE YOUR STRATEGY

Make a plan

Here, you build a plan that maps your aspirational goals to specific actions. A good plan helps ensure that your efforts map to the desired business outcomes.
Here are the steps in this stage.

Digital estate: Create an inventory of the existing digital assets and workloads that you plan to migrate to the cloud.	
Initial organizational alignment: Ensure that the right people are involved in your migration efforts, both from a technical standpoint as well as from a cloud governance standpoint.	
Skills readiness plan: Build a plan that helps individuals build the skills they need to operate in the cloud.	

Cloud adoption plan: Build a comprehensive plan that brings together the development, operations, and business teams toward a shared cloud adoption goal.	

MAKE A PLAN

Ready your organization

Here, you create a *landing zone*, or an environment in the cloud to begin hosting your workloads.
Here are the steps in this stage.

	Azure setup guide: Review the Azure setup guide to become familiar with the tools and approaches you need to use to create a landing zone.
	Azure landing zone: Begin to build out the Azure subscriptions that support each of the major areas of your business. A landing zone includes cloud infrastructure as well as governance, accounting, and security capabilities.
	Expand the landing zone: Refine your landing zone to ensure that it meets your operations, governance, and security needs.
	Best practices: Start with recommended and proven practices to help ensure that your cloud migration efforts are scalable and maintainable.

READY YOUR ORGANIZATION

Adopt the cloud

Here, you begin to migrate your applications to the cloud. Along the way, you might find ways to modernize your applications and build innovative solutions that use cloud services.
The Cloud Adoption Framework breaks this stage into two parts: migrate and innovate.
Migrate: Here are the steps in the migrate part of this stage.

Migrate your first workload: Use the Azure migration guide to deploy your first project to the cloud.	
Migration scenarios: Use additional in-depth guides to explore more complex migration scenarios.	
Best practices: Check in with the Azure cloud migration best practices checklist to verify	

that you're following recommended practices.	
Process improvements: Identify ways to make the migration process scale while requiring less effort.	

ADOPT THE CLOUD

Innovate: Here are the steps in the innovate part of this stage.

	Business value consensus: Verify that investments in new innovations add value to the business and meet customer needs.
	Azure innovation guide: Use this guide to accelerate development and build a minimum viable product (MVP) for your idea.
	Best practices: Verify that your progress maps to recommended practices before you move forward.
	Feedback loops: Check in frequently with your customers to verify that you're building what they need.

TABLE 5

Govern and manage your cloud environments

Here, you begin to form your cloud governance and cloud management strategies. As the cloud estate changes over time, so do cloud governance processes and policies. You need to create resilient solutions that are constantly optimized.

Govern: Here are the steps in the govern part of this stage.

Methodology: Consider your end state solution. Then define a methodology that incrementally takes you from your first steps all the way to full cloud governance.	
Benchmark: Use the governance benchmark tool to assess your current state and future state to establish a vision for applying the framework.	
Initial governance foundation: Create an MVP that captures the first steps of your	

governance plan.	
Improve the initial governance foundation: Iteratively add governance controls that address tangible risks as you progress toward your end state solution.	

GOVERN AND MANAGE YOUR CLOUD ENVIRONMENTS

Manage: Here are the steps in the manage part of this stage.

	Establish a management baseline: Define your minimum commitment to operations management. A management baseline is the minimum set of tools and processes that should be applied to every asset in an environment.
	Define business commitments: Document supported workloads to establish operational commitments with the business and agree on cloud management investments for each workload.
	Expand the management baseline: Apply recommended best practices to iterate on your initial management baseline.
	Advanced operations and design principles: For workloads that require a higher level of business commitment, perform a deeper architecture review to deliver on your resiliency and reliability commitments.

GOVERN AND MANAGE YOUR CLOUD ENVIRONMENTS

From <https://docs.microsoft.com/en-us/learn/modules/build-cloud-governance-strategy-azure/2-accelerate-cloud-adoption-framework>

Create a subscription governance strategy

- 3 minutes

In Plan and discuss Azure deployments, you learned that the organizing structure for resources in Azure has four levels: management groups, subscriptions, resource groups, and resources.

At the beginning of any cloud governance implementation, you identify a cloud organization structure that meets your business needs. This step often involves forming a *cloud center of excellence team* (also called a *cloud enablement team* or a *cloud custodian team*). This team is empowered to implement governance practices from a centralized location for the entire organization.

Teams often start their Azure governance strategy at the subscription level. There are three main aspects to consider when you create and manage subscriptions: billing, access control, and subscription limits.

Let's look at each of these aspects in more detail.

Billing

You can create one billing report per subscription. If you have multiple departments and need to do a "chargeback" of cloud costs, one possible solution is to organize subscriptions by department or by project.
Resource tags can also help. You'll explore tags later in this module. When you define how many subscriptions you need and what to name them, take into account your internal billing requirements.

Access control

A subscription is a deployment boundary for Azure resources. Every subscription is associated with an Azure Active Directory tenant. Each tenant provides administrators the ability to set granular access through defined roles by using Azure role-based access control.
When you design your subscription architecture, consider the deployment boundary factor. For example, do you need separate subscriptions for development and for production environments? With separate subscriptions, you can control access to each one separately and isolate their resources from one another.

Subscription limits

Subscriptions also have some resource limitations. For example, the maximum number of network Azure ExpressRoute circuits per subscription is 10. Those limits should be considered during your design phase. If you'll need to exceed those limits, you might need to add more subscriptions. If you hit a hard limit maximum, there's no flexibility to increase it.
Management groups are also available to assist with managing subscriptions. A management group manages access, policies, and compliance across multiple Azure subscriptions. You'll learn more about management groups later in this module.

From <https://docs.microsoft.com/en-us/learn/modules/build-cloud-governance-strategy-azure/3-create-subscription-governance-strategy>

Control access to cloud resources by using Azure role-based access control

- 4 minutes

When you have multiple IT and engineering teams, how can you control what access

they have to the resources in your cloud environment? It's a good security practice to grant users only the rights they need to perform their job, and only to the relevant resources.

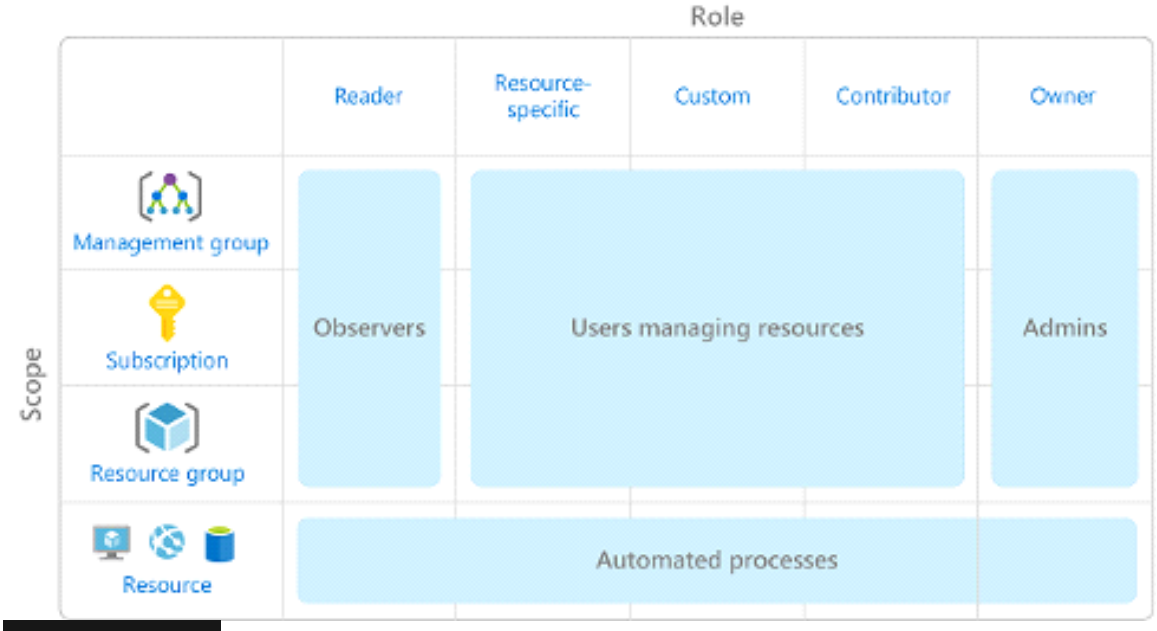
Instead of defining the detailed access requirements for each individual, and then updating access requirements when new resources are created, Azure enables you to control access through Azure role-based access control (Azure RBAC).

Azure provides built-in roles that describe common access rules for cloud resources. You can also define your own roles. Each role has an associated set of access permissions that relate to that role. When you assign individuals or groups to one or more roles, they receive all of the associated access permissions.

How is role-based access control applied to resources?

Role-based access control is applied to a *scope*, which is a resource or set of resources that this access applies to.

Here's a diagram that shows the relationship between roles and scopes.



Scopes include:

- A management group (a collection of multiple subscriptions).
- A single subscription.
- A resource group.
- A single resource.

Observers, *Users managing resources*, *Admins*, and *Automated processes* illustrate the kinds of users or accounts that would typically be assigned each of the various roles.

When you grant access at a parent scope, those permissions are inherited by all child scopes. For example:

- When you assign the Owner role to a user at the management group scope, that user can manage everything in all subscriptions within the management group.
- When you assign the Reader role to a group at the subscription scope, the members of that group can view every resource group and resource within the

subscription.
- When you assign the Contributor role to an application at the resource group scope, the application can manage resources of all types within that resource group, but not other resource groups within the subscription.

When should I use Azure RBAC?

Use Azure RBAC when you need to:
- Allow one user to manage VMs in a subscription and another user to manage virtual networks.
- Allow a database administrator group to manage SQL databases in a subscription.
- Allow a user to manage all resources in a resource group, such as virtual machines, websites, and subnets.
- Allow an application to access all resources in a resource group.

These are just a few examples. You'll find the complete list of built-in roles at the end of this module.

How is Azure RBAC enforced?

Azure RBAC is enforced on any action that's initiated against an Azure resource that passes through Azure Resource Manager. Resource Manager is a management service that provides a way to organize and secure your cloud resources.
You typically access Resource Manager from the Azure portal, Azure Cloud Shell, Azure PowerShell, and the Azure CLI. Azure RBAC doesn't enforce access permissions at the application or data level. Application security must be handled by your application.
RBAC uses an *allow model*. When you're assigned a role, RBAC *allows* you to perform certain actions, such as read, write, or delete. If one role assignment grants you read permissions to a resource group and a different role assignment grants you write permissions to the same resource group, you have both read and write permissions on that resource group.

Who does Azure RBAC apply to?

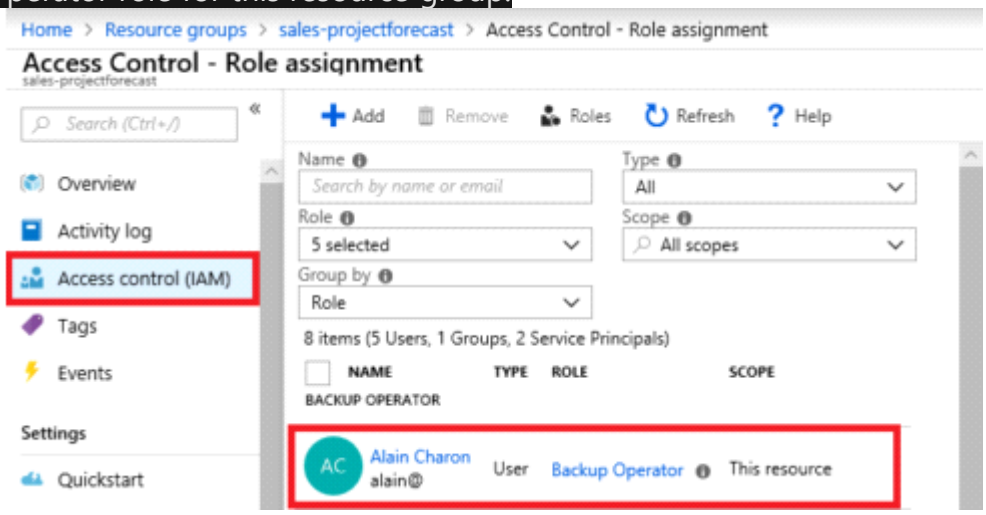
You can apply Azure RBAC to an individual person or to a group. You can also apply Azure RBAC to other special identity types, such as service principals and managed identities. These identity types are used by applications and services to automate access to Azure resources.
Tailwind Traders has the following teams with an interest in some part of their overall IT environment:
- IT Administrators
  This team has ultimate ownership of technology assets, both on-premises and in the cloud. The team requires full control of all resources.
- Backup and Disaster Recovery

This team is responsible for managing the health of regular backups and invoking any data or system recoveries.

- Cost and Billing
  People in this team track and report on technology-related spend. They also manage the organization's internal budgets.
- Security Operations
  This team monitors and responds to any technology-related security incidents. The team requires ongoing access to log files and security alerts.

How do I manage Azure RBAC permissions?

You manage access permissions on the Access control (IAM) pane in the Azure portal. This pane shows who has access to what scope and what roles apply. You can also grant or remove access from this pane.
The following screenshot shows an example of the Access control (IAM) pane for a resource group. In this example, Alain Charon has been assigned the Backup Operator role for this resource group.



From <https://docs.microsoft.com/en-us/learn/modules/build-cloud-governance-strategy-azure/4-control-access-azure-rbac>

Prevent accidental changes by using resource locks

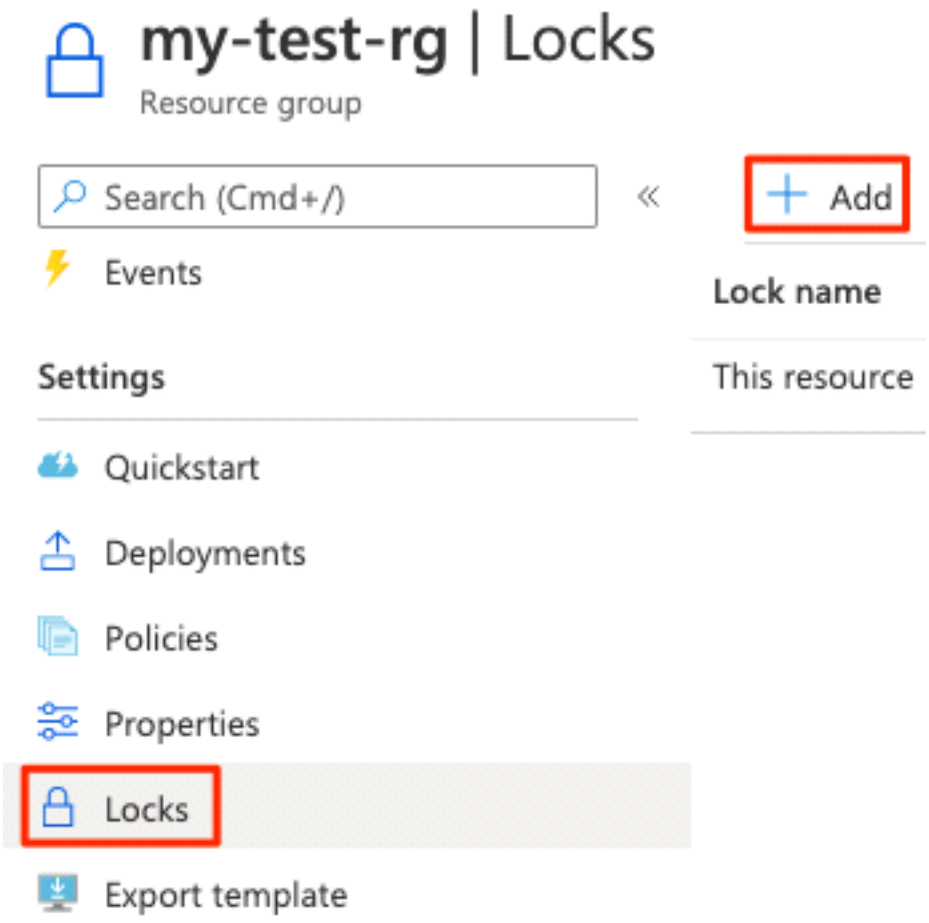
- 3 minutes

A resource lock prevents resources from being accidentally deleted or changed. Even with Azure role-based access control (Azure RBAC) policies in place, there's still a risk that people with the right level of access could delete critical cloud resources. Think of a resource lock as a warning system that reminds you that a resource should not be deleted or changed.
For example, at Tailwind Traders, an IT administrator was performing routine cleanup of unused resources in Azure. The admin accidentally deleted resources that appeared to be unused. But these resources were critical to an application that's used for seasonal

promotions. How can resource locks help prevent this kind of incident from happening in the future?

How do I manage resource locks?

You can manage resource locks from the Azure portal, PowerShell, the Azure CLI, or from an Azure Resource Manager template.
To view, add, or delete locks in the Azure portal, go to the Settings section of any resource's Settings pane in the Azure portal.
Here's an example that shows how to add a resource lock from the Azure portal. You'll apply a similar resource lock in the next part.



What levels of locking are available?

You can apply locks to a subscription, a resource group, or an individual resource. You can set the lock level to CanNotDelete or ReadOnly.

- CanNotDelete means authorized people can still read and modify a resource, but they can't delete the resource without first removing the lock.
- ReadOnly means authorized people can read a resource, but they can't delete or change the resource. Applying this lock is like restricting all authorized users to the permissions granted by the Reader role in Azure RBAC.

How do I delete or change a locked resource?

Although locking helps prevent accidental changes, you can still make changes by following a two-step process.
To modify a locked resource, you must first remove the lock. After you remove the lock, you can apply any action you have permissions to perform. This additional step allows the action to be taken, but it helps protect your administrators from doing something they might not have intended to do.
Resource locks apply regardless of RBAC permissions. Even if you're an owner of the resource, you must still remove the lock before you can perform the blocked activity.

Combine resource locks with Azure Blueprints

What if a cloud administrator accidentally deletes a resource lock? If the resource lock is removed, its associated resources can be changed or deleted.
To make the protection process more robust, you can combine resource locks with Azure Blueprints. Azure Blueprints enables you to define the set of standard Azure resources that your organization requires. For example, you can define a blueprint that specifies that a certain resource lock must exist. Azure Blueprints can automatically replace the resource lock if that lock is removed.
You'll learn more about Azure Blueprints later in this module.

From <https://docs.microsoft.com/en-us/learn/modules/build-cloud-governance-strategy-azure/5-prevent-changes-resource-locks>

Exercise - Protect a storage account from accidental deletion by using a resource lock

- 8 minutes

In this exercise, you see how resource locks help prevent accidental deletion of your Azure resources.
To do so, you create a resource group from the Azure portal. Think of a resource group as a container for related Azure resources. Then you add a lock to your resource group and verify that you can't delete the resource group.
You then add a storage account to your resource group and see how the lock from the parent resource group prevents the storage account from being deleted. A storage account is a container that groups a set of Azure Storage services together.

Important

You need your own Azure subscription to complete the exercises in this module. If you don't have an Azure subscription, you can still read along.

Create the resource group

Here you create a resource group that's named my-test-rg.

1. Go to the Azure portal and sign in.
2. At the top of the page, select Resource groups.
3. Select + New. The Create a resource group page appears.
4. In the Basics tab, fill in the following fields.

Setting	Value
Project details	
Subscription	*Your Azure subscription*
Resource group	my-test-rg
Resource details	
Region	(US) East US

TABLE 1

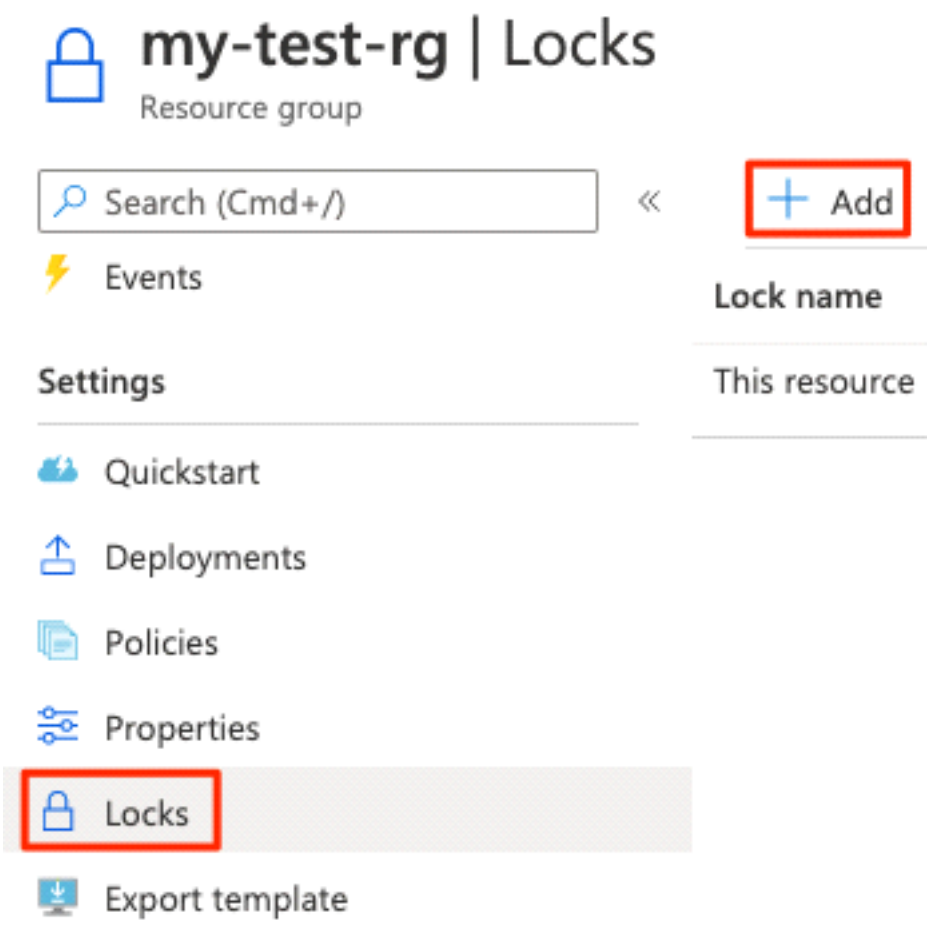
You can also select a region that's closer to you.

5. Select Review + create, and then select Create.

Add a lock to the resource group

Add a resource lock to the resource group. To do so:

1. From the Azure portal, select your resource group, my-test-rg.
2. Under Settings, select Locks, and then select Add.

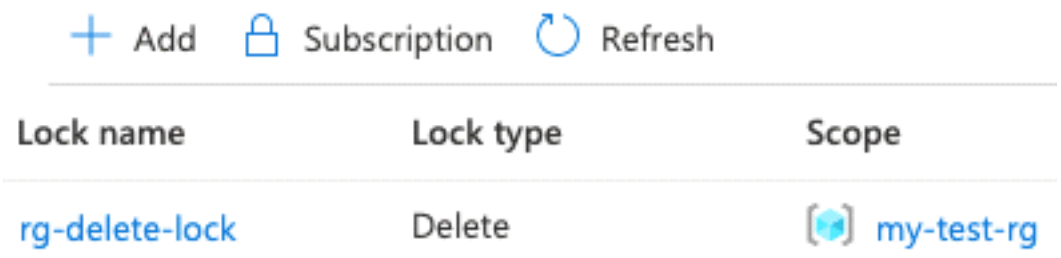


3. Fill in these fields.

Setting	Value
Lock name	rg-delete-lock
Lock type	Delete

TABLE 2

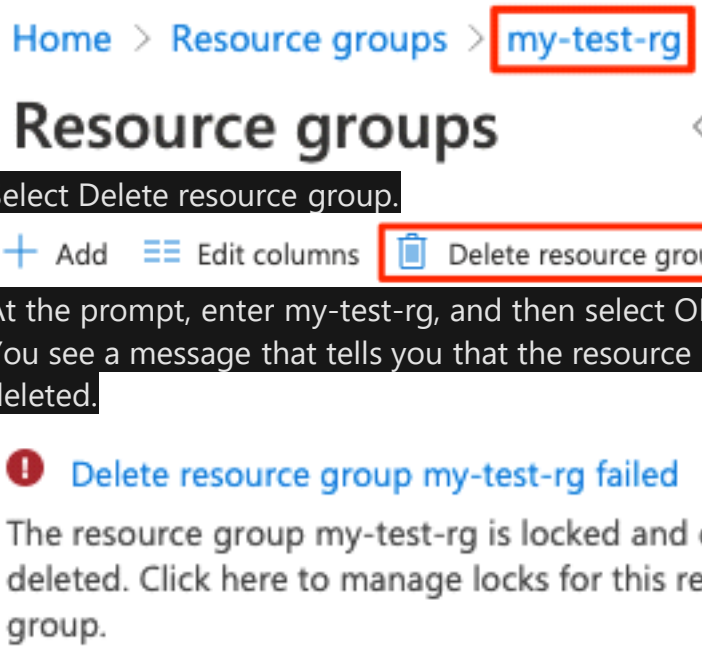
4. Select OK.
You see that the resource lock is applied to your resource group.



Verify that the resource group is protected from deletion

Here, you verify protection by attempting to delete the resource group.

1. From the top of the page, select my-test-rg to go to your resource group's overview page.



2. Select Delete resource group.
3. At the prompt, enter my-test-rg, and then select OK.
You see a message that tells you that the resource group is locked and can't be deleted.

Protect a storage account from accidental deletion

Here, you add a storage account to your resource group and see how the lock from the parent resource group prevents the storage account from being deleted. To do so:

1. From the Azure portal, at the top of the page, select Home to return to the start page.
2. Select Storage accounts. Then select + New. The Create storage account page appears.
3. In the Basics tab, fill in the following fields.
Note
Replace NNN with a series of numbers. The numbers help to ensure that your storage account name is unique.

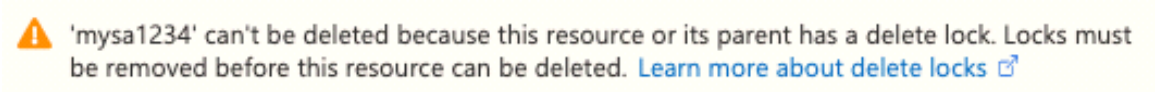
Setting	Value
Project details	
Subscription	*Your Azure subscription*
Resource group	my-test-rg
Instance details	
Storage account name	mysaNNN
Location	(US) East US
Performance	Standard
Account kind	StorageV2 (general purpose v2)
Replication	Locally redundant storage (LRS)

TABLE 3

As before, you can also select a region that's closer to you.
4. Select Review + create, and then select Create.
The deployment might take a few moments to complete.

5. Select Go to resource.
6. At the top of the page, select Delete.

You see a message that tells you the resource or its parent is locked and can't be deleted. Here's an example that shows the error message for a storage account that's named mysa1234.



Although you didn't create a lock specifically for the storage account, the lock you created for the parent resource group prevents you from deleting the resource. In other words, the storage account inherits the lock from the parent resource group.

Delete the resource group and the storage account

You no longer need your resource group or storage account. Here you remove both. When you delete a resource group, you also delete its child resources, such as the storage account you previously created.
To delete the resource group, you first need to remove the resource lock.

1. From the Azure portal, select Home > Resource groups > my-test-rg to go to your resource group.
2. Under Settings, select Locks.
3. Locate rg-delete-lock, and select Delete on that same row.
4. Select Overview, and then select Delete resource group.
5. At the prompt, enter my-test-rg, and then select OK.
   The deletion operation might take a few moments to complete.
6. When the operation completes, select Home > Resource groups.
   You see that the my-test-rg resource group no longer exists in your account. Your storage account is also deleted.

Nice work. You can now apply resource locks to help prevent the accidental deletion of your Azure resources.

From <https://docs.microsoft.com/en-us/learn/modules/build-cloud-governance-strategy-azure/6-protect-storage-account-resource-lock>

Organize your Azure resources by using tags

- 3 minutes

As your cloud usage grows, it's increasingly important to stay organized. A good organization strategy helps you understand your cloud usage and can help you manage costs.
For example, as Tailwind Traders prototypes new ways to deploy its applications on Azure, it needs a way to mark its test environments so that it can easily identify and

delete resources in these environments when they're no longer needed.

One way to organize related resources is to place them in their own subscriptions. You can also use resource groups to manage related resources. Resource *tags* are another way to organize resources. Tags provide extra information, or metadata, about your resources. This metadata is useful for:

- Resource management
  Tags enable you to locate and act on resources that are associated with specific workloads, environments, business units, and owners.
- Cost management and optimization
  Tags enable you to group resources so that you can report on costs, allocate internal cost centers, track budgets, and forecast estimated cost.
- Operations management
  Tags enable you to group resources according to how critical their availability is to your business. This grouping helps you formulate service-level agreements (SLAs). An SLA is an uptime or performance guarantee between you and your users.
- Security
  Tags enable you to classify data by its security level, such as *public* or *confidential*.
- Governance and regulatory compliance
  Tags enable you to identify resources that align with governance or regulatory compliance requirements, such as ISO 27001.
  Tags can also be part of your standards enforcement efforts. For example, you might require that all resources be tagged with an owner or department name.
- Workload optimization and automation
  Tags can help you visualize all of the resources that participate in complex deployments. For example, you might tag a resource with its associated workload or application name and use software such as Azure DevOps to perform automated tasks on those resources.

How do I manage resource tags?

You can add, modify, or delete resource tags through PowerShell, the Azure CLI, Azure Resource Manager templates, the REST API, or the Azure portal.

You can also manage tags by using Azure Policy. For example, you can apply tags to a resource group, but those tags aren't automatically applied to the resources within that resource group. You can use Azure Policy to ensure that a resource inherits the same tags as its parent resource group. You'll learn more about Azure Policy later in this module.

You can also use Azure Policy to enforce tagging rules and conventions. For example, you can require that certain tags be added to new resources as they're provisioned. You can also define rules that reapply tags that have been removed.

An example tagging structure

A resource tag consists of a name and a value. You can assign one or more tags to each

Azure resource.
After reviewing its business requirements, Tailwind Traders decides on the following tags.

Name	Value
AppName	The name of the application that the resource is part of.
CostCenter	The internal cost center code.
Owner	The name of the business owner who's responsible for the resource.
Environment	An environment name, such as "Prod," "Dev," or "Test."
Impact	How important the resource is to business operations, such as "Mission-critical," "High-impact," or "Low-impact."

AN EXAMPLE TAGGING STRUCTURE
Here's an example that shows these tags as they're applied to a virtual machine during provisioning.

Name		Value	Resource
AppName	:	SpecialOrders	Virtual machine
CostCenter	:	0224 - Infrastructure R&D	Virtual machine
Owner	:	tim@tailwindtraders.com	Virtual machine
Environment	:	Test	Virtual machine
Impact	:	High-impact	Virtual machine

The Tailwind Traders team can run queries, for example, from PowerShell or the Azure CLI, to list all resources that contain these tags.
Keep in mind that you don't need to enforce that a specific tag is present on all of your resources. For example, you might decide that only mission-critical resources have the Impact tag. All non-tagged resources would then not be considered as mission-critical.

From <https://docs.microsoft.com/en-us/learn/modules/build-cloud-governance-strategy-azure/7-organize-resource-tags>

Control and audit your resources by using Azure Policy

- 5 minutes

Now that you've identified your governance and business requirements, how do you ensure that your resources *stay* compliant? How can you be alerted if a resource's configuration has changed?
Azure Policy is a service in Azure that enables you to create, assign, and manage policies that control or audit your resources. These policies enforce different rules and effects over your resource configurations so that those configurations stay compliant

with corporate standards.

How does Azure Policy define policies?

Azure Policy enables you to define both individual policies and groups of related policies, known as *initiatives*. Azure Policy evaluates your resources and highlights resources that aren't compliant with the policies you've created. Azure Policy can also prevent noncompliant resources from being created.

Azure Policy comes with a number of built-in policy and initiative definitions that you can use, under categories such as Storage, Networking, Compute, Security Center, and Monitoring.

For example, say you define a policy that allows only a certain stock-keeping unit (SKU) size of virtual machines (VMs) to be used in your environment. After you enable this policy, that policy is applied when you create new VMs or resize existing VMs. Azure Policy also evaluates any current VMs in your environment.

In some cases, Azure Policy can automatically remediate noncompliant resources and configurations to ensure the integrity of the state of the resources. For example, if all resources in a certain resource group should be tagged with the AppName tag and a value of "SpecialOrders," Azure Policy can automatically reapply that tag if it has been removed.

Azure Policy also integrates with Azure DevOps by applying any continuous integration and delivery pipeline policies that apply to the pre-deployment and post-deployment phases of your applications.

Azure Policy in action

Implementing a policy in Azure Policy involves these three steps:

1. Create a policy definition.
2. Assign the definition to resources.
3. Review the evaluation results.

Let's examine each step in more detail.

1. Create a policy definition

A policy definition expresses what to evaluate and what action to take. For example, you could prevent VMs from being deployed in certain Azure regions. You also could audit your storage accounts to verify that they only accept connections from allowed networks.

Every policy definition has conditions under which it's enforced. A policy definition also has an accompanying effect that takes place when the conditions are met. Here are some example policy definitions:

- Allowed virtual machine SKUs
  This policy enables you to specify a set of VM SKUs that your organization can

deploy.

- Allowed locations
  This policy enables you to restrict the locations that your organization can specify when it deploys resources. Its effect is used to enforce your geographic compliance requirements.
- MFA should be enabled on accounts with write permissions on your subscription
  This policy requires that multifactor authentication (MFA) be enabled for all subscription accounts with write privileges to prevent a breach of accounts or resources.
- CORS should not allow every resource to access your web applications
  Cross-origin resource sharing (CORS) is an HTTP feature that enables a web application running under one domain to access resources in another domain. For security reasons, modern web browsers restrict cross-site scripting by default. This policy allows only required domains to interact with your web app.
- System updates should be installed on your machines
  This policy enables Azure Security Center to recommend missing security system updates on your servers.

2. Assign the definition to resources

To implement your policy definitions, you assign definitions to resources. A *policy assignment* is a policy definition that takes place within a specific scope. This scope could be a management group (a collection of multiple subscriptions), a single subscription, or a resource group.
Policy assignments are inherited by all child resources within that scope. If a policy is applied to a resource group, that policy is applied to all resources within that resource group. You can exclude a subscope from the policy assignment if there are specific child resources you need to be exempt from the policy assignment.

3. Review the evaluation results

When a condition is evaluated against your existing resources, each resource is marked as compliant or noncompliant. You can review the noncompliant policy results and take any action that's needed.
Policy evaluation happens about once per hour. If you make changes to your policy definition and create a policy assignment, that policy is evaluated over your resources within the hour.

What are Azure Policy initiatives?

An Azure Policy initiative is a way of grouping related policies into one set. The initiative definition contains all of the policy definitions to help track your compliance state for a larger goal.

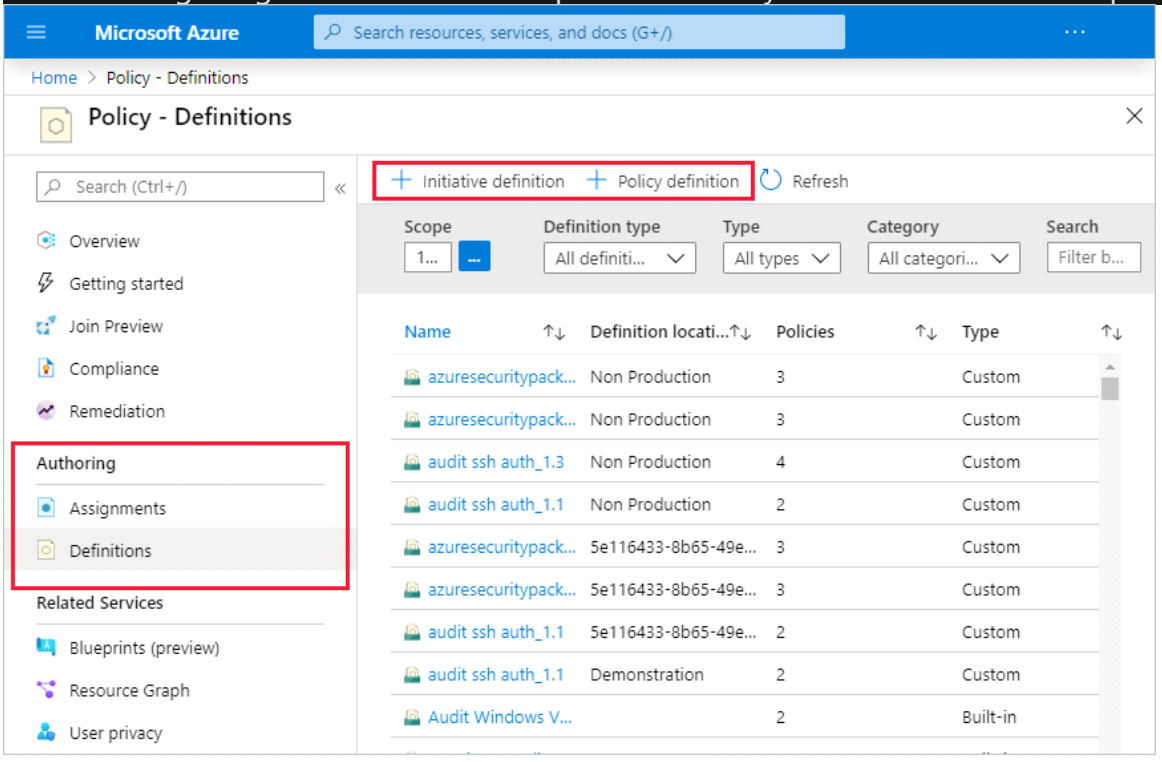
For example, Azure Policy includes an initiative named Enable Monitoring in Azure Security Center. Its goal is to monitor all of the available security recommendations for all Azure resource types in Azure Security Center.
Under this initiative, the following policy definitions are included:

- Monitor unencrypted SQL Database in Security Center
  This policy monitors for unencrypted SQL databases and servers.
- Monitor OS vulnerabilities in Security Center
  This policy monitors servers that don't satisfy the configured OS vulnerability baseline.
- Monitor missing Endpoint Protection in Security Center
  This policy monitors for servers that don't have an installed endpoint protection agent.

In fact, the Enable Monitoring in Azure Security Center initiative contains over 100 separate policy definitions.
Azure Policy also includes initiatives that support regulatory compliance standards such as HIPAA and ISO 27001.

How do I define an initiative?

You define initiatives by using the Azure portal or by using command-line tools. From the Azure portal, you can search the list of built-in initiatives that are already provided by Azure. You also can create your own custom policy definition.
The following image shows a few example Azure Policy initiatives in the Azure portal.



How do I assign an initiative?

Like a policy assignment, an initiative assignment is an initiative definition that's assigned to a specific scope of a management group, a subscription, or a resource group.
Even if you have only a single policy, an initiative enables you to increase the number of policies over time. Because the associated initiative remains assigned, it's easier to add and remove policies without the need to change the policy assignment for your resources.

From <https://docs.microsoft.com/en-us/learn/modules/build-cloud-governance-strategy-azure/8-control-audit-resources-azure-policy>

Exercise - Restrict deployments to a specific location by using Azure Policy

- 8 minutes

In this exercise, you create a policy in Azure Policy that restricts the deployment of Azure resources to a specific location. You verify the policy by attempting to create a storage account in a location that violates the policy.
Tailwind Traders wants to limit the location where resources can be deployed to the East US region. It has two reasons:

- Improved cost tracking
  To track costs, Tailwind Traders uses different subscriptions to track deployments to each of its regional locations. The policy will ensure that all resources are deployed to the East US region.
- Adhere to data residency and security compliance
  Tailwind Traders must adhere to a compliance rule that states where customer data can be stored. Here, customer data must be stored in the East US region.

Recall that you can assign a policy to a management group, a single subscription, or a resource group. Here, you assign the policy to a resource group so that policy doesn't affect any other resources in your Azure subscription.

Important
You need your own Azure subscription to complete the exercises in this module. If you don't have an Azure subscription, you can still read along.

Create the resource group

Here you create a resource group that's named my-test-rg. This is the resource group to which you'll apply your location policy.
For learning purposes, you use the same resource group name that you used in the previous exercise. You can use the same name because you deleted the previous resource group.

1. Go to the Azure portal, and sign in.

2. Select Create a resource.
3. Enter resource group in the search box, and select Enter.
4. If you're taken to a search results page, select Resource group from the results.
5. Select Create. Then fill in these fields.

Setting	Value
Subscription	*(Your Azure subscription)*
Subscription > Resource group	my-test-rg
Region	(US) East US

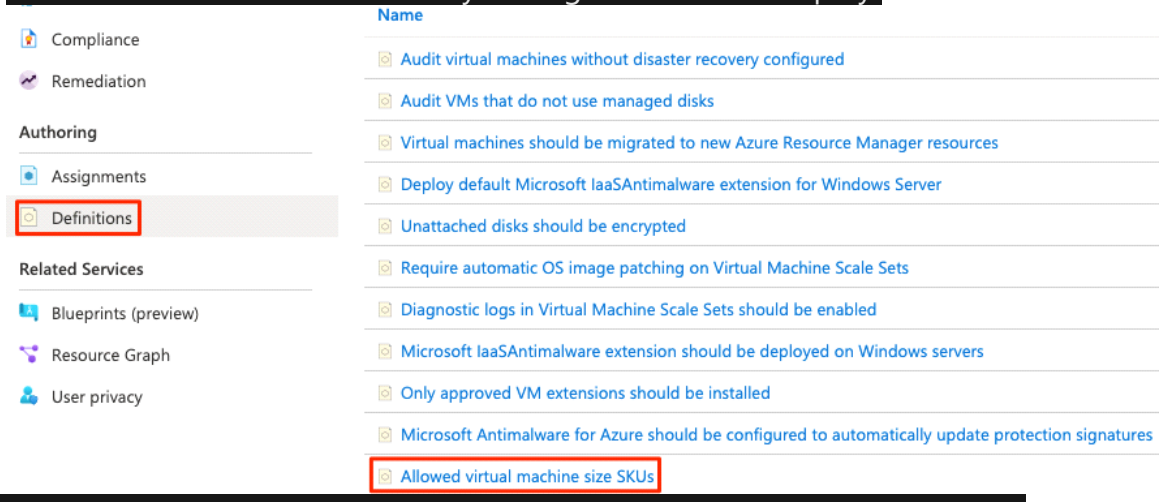
TABLE 1

6. Select Review + create, and then select Create.

Explore predefined policies

Before you configure your location policy, let's take a brief look at some predefined policies. As an example, you'll look at policies that relate to Azure Compute services.

1. From the Azure portal, at the top of the page, select Home to return to the start page.
2. At the top of the page, enter policy in the search bar. Then select Policy from the list of results to access Azure Policy.
3. Under Authoring, select Definitions.
4. From the Category drop-down list, select only Compute.
   Notice that the Allowed virtual machine SKUs definition enables you to specify a set of virtual machine SKUs that your organization can deploy.

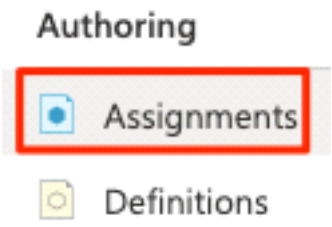


As an optional step, explore any other policies or categories that interest you.

Configure the location policy

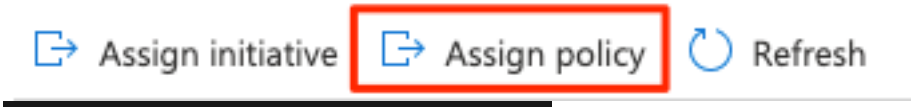
Here you configure the allowed location policy by using Azure Policy. Then you assign that policy to your resource group. To do so:

1. From the Policy page, under Authoring, select Assignments.



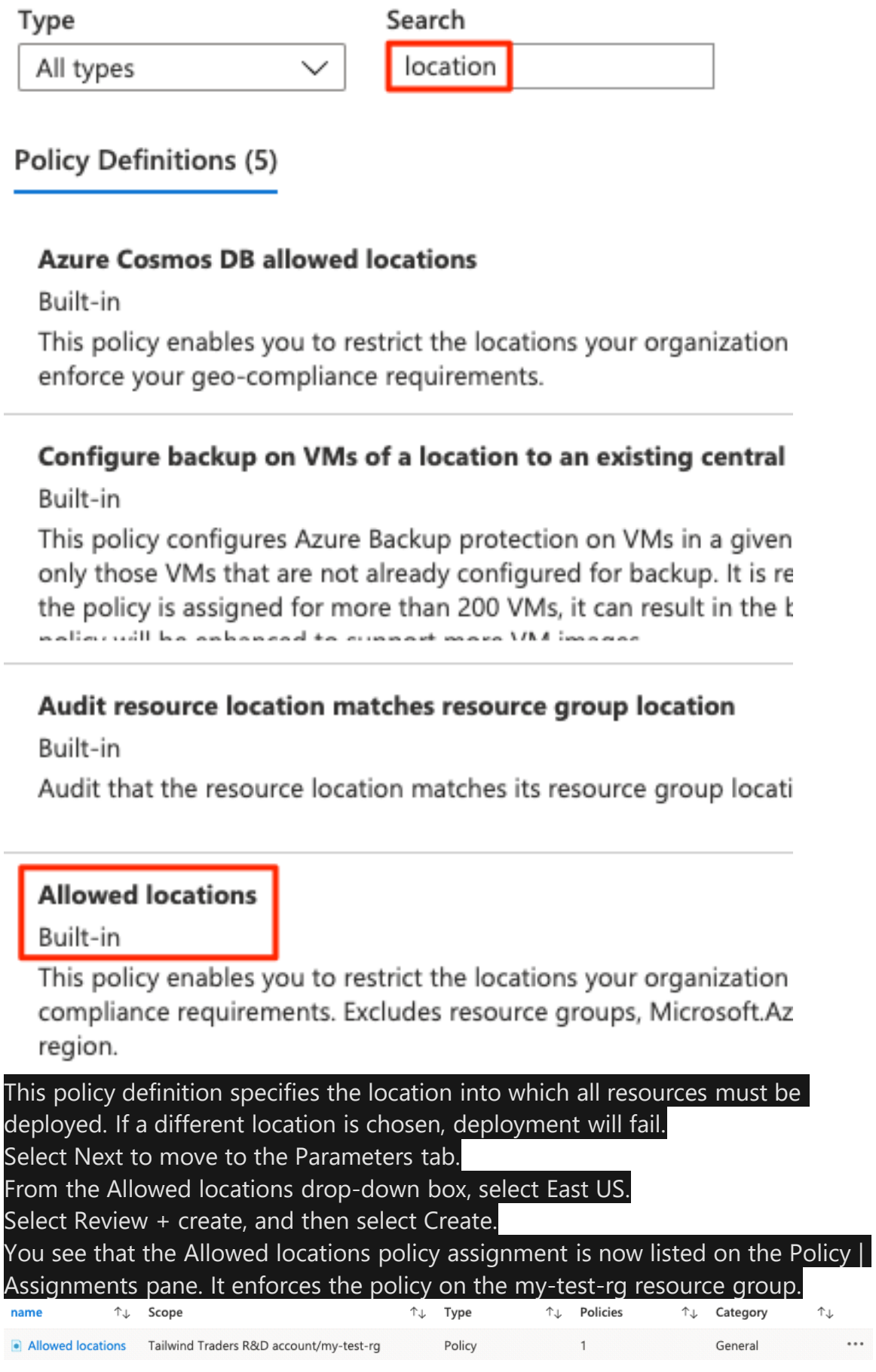
An assignment is a policy that has been assigned to take place within a specific scope. For example, a definition could be assigned to the subscription scope.

2. Select Assign Policy.



You're taken to the Assign policy page.

3. Under Scope, select the ellipsis.
   From the dialog box that appears, set:
4. The Subscription field to your Azure subscription.
5. The Resource Group field to my-test-rg.
6. Select the Select button.
7. Under Policy definition, select the ellipsis.
8. In the search bar, enter location.
9. Select the Allowed locations definition.
10. Select the Select button.



This policy definition specifies the location into which all resources must be deployed. If a different location is chosen, deployment will fail.

11. Select Next to move to the Parameters tab.
12. From the Allowed locations drop-down box, select East US.
13. Select Review + create, and then select Create.

You see that the Allowed locations policy assignment is now listed on the Policy | Assignments pane. It enforces the policy on the my-test-rg resource group.

Verify the location policy

Here you attempt to add a storage account to your resource group at a location that violates your location policy.

1. From the Azure portal, at the top of the page, select Home to return to the start page.
2. Select Create a resource.
3. Enter storage account in the search box, and select Enter.
4. If you're taken to a search results page, select Storage account from the results.
5. Select Create. Then fill in these fields.

   Note

   Replace NNN with a series of numbers. Numbers help to ensure that your storage account name is unique.

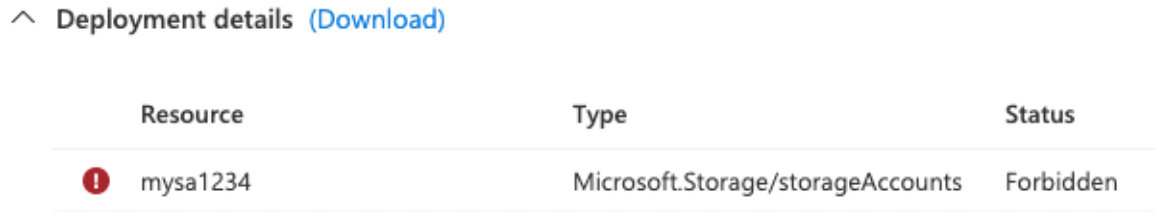
Setting	Value
Subscription	*(Your Azure subscription)*
Subscription > Resource group	my-test-rg
Storage account name	mysaNNN
Location	(Asia Pacific) Japan East
Performance	Standard
Account kind	StorageV2 (general purpose v2)
Replication	Locally redundant storage (LRS)
Access tier (default)	Hot

TABLE 2

   If you previously selected Japan East in your location policy, select a different region from the list.
6. Select Review + create, and then select Create.

   You see a message that states that the deployment failed because of the policy violation. You also see the deployment details.

   Here's an example that shows the deployment details for a storage account named mysa1234.

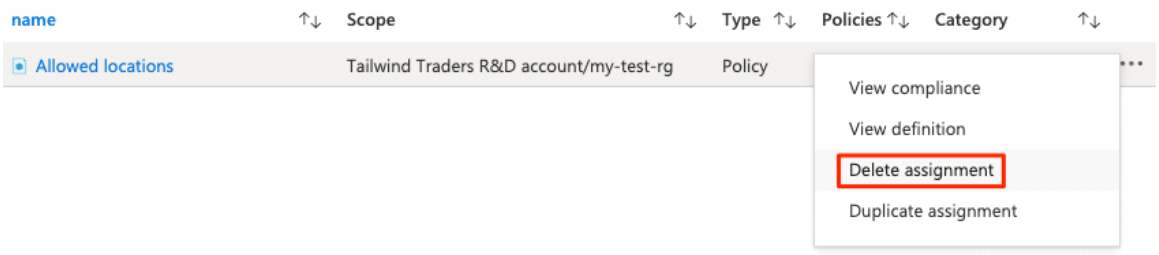


Delete the policy assignment

You no longer need your policy assignment. Here you remove it from your subscription.

1. From the Azure portal, select Home > Policy.
2. Under Authoring, select Assignments.
3. On the Allowed locations row, select the ellipsis. Then select Delete assignment.

When prompted, select Yes.



You see that the Allowed locations policy assignment no longer exists.

As an optional step, you can try to create the storage account a second time to verify that the policy is no longer in effect.

Delete the resource group

You no longer need your resource group. Here you remove it from your subscription.

1. From the Azure portal, select Home > Resource groups > my-test-rg to go to your resource group.
2. Select Overview, and then select Delete resource group.
3. At the prompt, enter my-test-rg, and then select OK.
   The deletion operation might take a few moments to complete.
4. After the operation completes, select Home > Resource groups.
   You see that the my-test-rg resource group no longer exists in your account.

Great work! You've successfully applied a policy by using Azure Policy to restrict the deployment of Azure resources to a specific location. You can now apply the policies that you need at the management group, subscription, or resource group level.

From <https://docs.microsoft.com/en-us/learn/modules/build-cloud-governance-strategy-azure/9-restrict-location-azure-policy>

Govern multiple subscriptions by using Azure Blueprints

- 4 minutes

So far, you've explored a number of Azure features that can help you implement your governance decisions, monitor the compliance of your cloud resources, and control access and protect critical resources from accidental deletion.

What happens when your cloud environment starts to grow beyond just one subscription? How can you scale the configuration of these features, knowing they need to be enforced for resources in new subscriptions?

Instead of having to configure features like Azure Policy for each new subscription, with Azure Blueprints you can define a repeatable set of governance tools and standard Azure resources that your organization requires. In this way, development teams can rapidly build and deploy new environments with the knowledge that they're building within organizational compliance with a set of built-in components that speed the development and deployment phases.

Azure Blueprints orchestrates the deployment of various resource templates and other artifacts, such as:

- Role assignments
- Policy assignments
- Azure Resource Manager templates
- Resource groups

Azure Blueprints in action

When you form a cloud center of excellence team or a cloud custodian team, that team can use Azure Blueprints to scale their governance practices throughout the organization.

Implementing a blueprint in Azure Blueprints involves these three steps:

1. Create an Azure blueprint.
2. Assign the blueprint.
3. Track the blueprint assignments.

With Azure Blueprints, the relationship between the blueprint definition (what should be deployed) and the blueprint assignment (what was deployed) is preserved. In other words, Azure creates a record that associates a resource with the blueprint that defines it. This connection helps you track and audit your deployments.

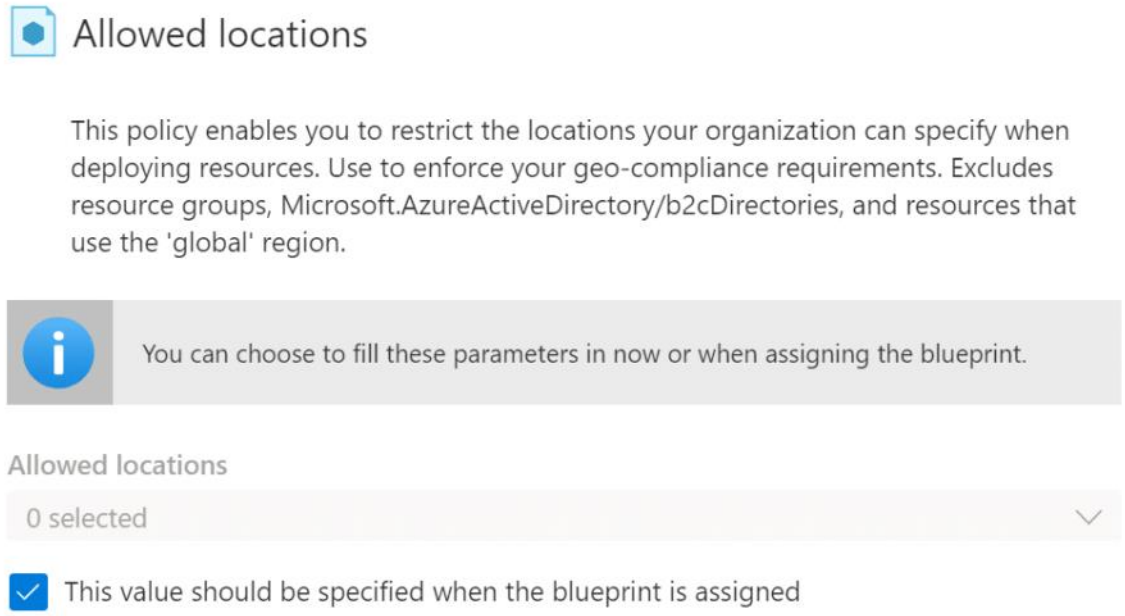
Blueprints are also versioned. Versioning enables you to track and comment on changes to your blueprint.

What are blueprint artifacts?

Each component in the blueprint definition is known as an *artifact*.

Artifacts can have no parameters. An example is the Deploy threat detection on SQL servers policy, which requires no further configuration.

Artifacts can also contain one or more parameters that you can configure. The following screenshot shows the Allowed locations policy. This policy includes a parameter that specifies the allowed locations.



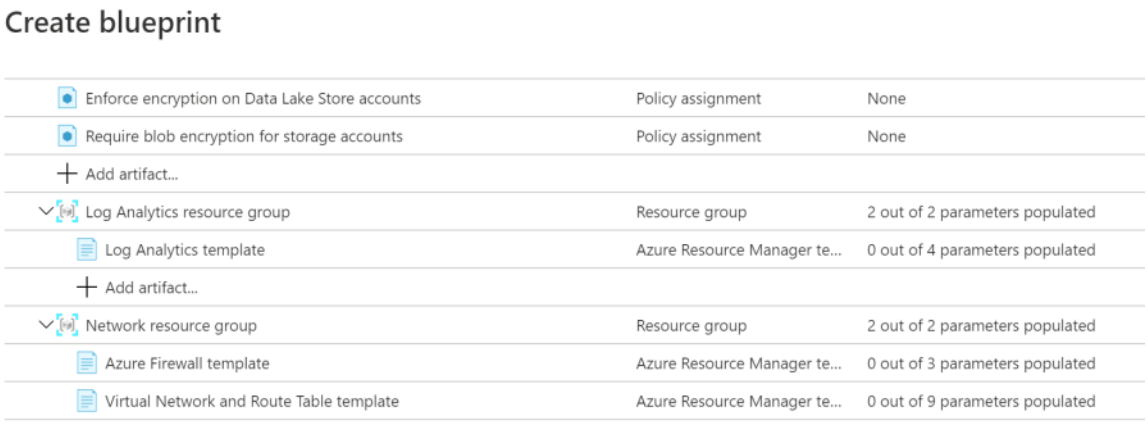
You can specify a parameter's value when you create the blueprint definition or when you assign the blueprint definition to a scope. In this way, you can maintain one standard blueprint but have the flexibility to specify the relevant configuration parameters at each scope where the definition is assigned.

How will Tailwind Traders use Azure Blueprints for ISO 27001 compliance?

ISO 27001 is a standard that applies to the security of IT systems, published by the International Organization for Standardization. As part of its quality process, Tailwind Traders wants to certify that it complies with this standard. Azure Blueprints has several built-in blueprint definitions that relate to ISO 27001.
As an IT administrator, you decide to investigate the ISO 27001: Shared Services Blueprint definition. Here's an outline of your plan.

1. Define a management group that's named PROD-MG.
   Recall that a management group manages access, policies, and compliance across multiple Azure subscriptions. Every new Azure subscription is added to this management group when the subscription is created.
2. Create a blueprint definition that's based on the ISO 27001: Shared Services Blueprint template. Then publish the blueprint.
3. Assign the blueprint to your PROD-MG management group.

The following image shows artifacts that are created when you run an ISO 27001 blueprint from a template.



You see that the blueprint template contains policy assignments, Resource Manager templates, and resource groups. The blueprint deploys these artifacts to any existing subscriptions within the PROD-MG management group. The blueprint also deploys these artifacts to any new subscriptions as they're created and added to the management group.

From <https://docs.microsoft.com/en-us/learn/modules/build-cloud-governance-strategy-azure/10-govern-subscriptions-azure-blueprints>

Examine privacy, compliance, and data protection standards on Azure

Thursday, January 28, 2021 10:54 AM

Learn about Microsoft's commitment to privacy and how Azure adheres to common regulatory and compliance standards.

Overview

- Introduction 4 min
- Explore compliance terms and requirements 5 min
- Access the Microsoft Privacy Statement, the Online Services Terms, and the Data Protection Addendum 3 min
- Explore the Trust Center 3 min
- Access Azure compliance documentation 4 min
- What is Azure Government? 2 min
- What is Azure China 21Vianet? 2 min
- Knowledge check 3 min
- Summary 1 min

From <https://docs.microsoft.com/en-us/learn/paths/az-900-describe-identity-governance-privacy-compliance-features/>

Introduction

- 4 minutes

In this module, you'll learn about Microsoft's commitment to privacy and how Azure adheres to common regulatory and compliance standards.

If your organization is a government department or agency, or you need to deploy to regions of China, you'll also learn about some considerations that don't apply to other Azure users.

In general, *compliance* means to adhere to a law, standard, or set of guidelines. *Regulatory compliance* refers to the discipline and process of ensuring that a company follows the laws that governing bodies enforce.

Meet Tailwind Traders

Tailwind Traders is a fictitious home improvement retailer. It operates retail hardware stores across the globe and online.

Tailwind Traders specializes in competitive pricing, fast shipping, and a large range of items. It's looking at cloud technologies to improve business operations and support growth into new markets. By moving to the cloud, the company plans to enhance its shopping experience to further differentiate itself from competitors.

How will Tailwind Traders protect its data in the cloud and stay compliant?

Tailwind Traders is planning its migration to the cloud. It's used to having full control of all of its application data, which is stored on servers that it manages in its datacenter.

Tailwind Traders knows that moving an application to the cloud means that data is now outside of its own walls. The company also understands that the cloud provider has access to the server hardware and infrastructure. How is the privacy of its application data protected?
Tailwind Traders must also adhere to multiple regulatory and compliance frameworks. For example, it must follow certain rules to ensure that it properly handles credit card data. It will still need to ensure that its applications comply with applicable regulations and standards. How does infrastructure on Azure already adhere to these same standards?
To answer these questions, you'll start by learning about the types of compliance offerings that are available on Azure.

Learning objectives

After completing this module, you'll be able to:

- Explain the types of compliance offerings that are available on Azure.
- Access the Microsoft Privacy Statement, the Online Services Terms, and the Data Protection Addendum to learn what personal data Microsoft collects, how Microsoft uses it, and for what purposes.
- Gain insight into regulatory standards and compliance on Azure from the Trust Center and from the Azure compliance documentation.
- Explain Azure capabilities that are specific to government agencies.

Prerequisites

- You should be familiar with basic computing concepts and terminology.
- Familiarity with cloud computing is helpful but isn't necessary.

From <https://docs.microsoft.com/en-us/learn/modules/examine-privacy-compliance-data-protection-standards/1-introduction>

Explore compliance terms and requirements

- 5 minutes

In this unit, you learn about the types of compliance offerings that are available on Azure.
As Tailwind Traders moves to running its applications in the cloud, it wants to know how Azure adheres to applicable regulatory compliance frameworks. The company asks:

- How compliant is Azure when it comes to handling personal data?
- How compliant are each of Azure's individual services?

Microsoft's online services build upon a common set of regulatory and compliance controls. Think of a *control* as a known good standard that you can compare your solution against to ensure security. These controls address today's regulations and adapt as regulations evolve.

Which compliance categories are available on Azure?

Although there are many more, the following image shows some of the more popular compliance offerings that are available on Azure. These offerings are grouped under four categories: Global, US Government, Industry, and Regional.

To get a sense of the variety of the compliance offerings available on Azure, let's take a closer look at a few of them.
While not all of these compliance offerings will be relevant to you or your team, they show that Microsoft's commitment to compliance is comprehensive, ongoing, and independently tested and verified.

Criminal Justice Information Service

Any US state or local agency that wants to access the FBI's Criminal Justice Information Services (CJIS) database is required to adhere to the CJIS Security Policy.
Azure is the only major cloud provider that contractually commits to conformance with the CJIS Security Policy. Microsoft adheres to the same requirements that law enforcement and public safety entities must meet.

Cloud Security Alliance STAR Certification

Azure, Intune, and Microsoft Power BI have obtained Cloud Security Alliance (CSA) STAR Certification, which involves a rigorous independent third-party assessment of a cloud provider's security posture.
STAR Certification is based on achieving International Organization of Standards/International Electrotechnical Commission (ISO/IEC) 27001 certification and meeting criteria specified in the Cloud Controls Matrix (CCM). This certification demonstrates that a cloud service provider:

- Conforms to the applicable requirements of ISO/IEC 27001.
- Has addressed issues critical to cloud security as outlined in the CCM.
- Has been assessed against the STAR Capability Maturity Model for the management of activities in CCM control areas.

European Union Model Clauses

Microsoft offers customers European Union (EU) Standard Contractual Clauses that provide contractual guarantees around transfers of personal data outside of the EU.
Microsoft is the first company to receive joint approval from the EU's Article 29 Working Party that the contractual privacy protections Azure delivers to its enterprise cloud customers meet current EU standards for international transfers of data. Meeting this standard ensures that Azure customers can use Microsoft services to move data freely through Microsoft's cloud, from Europe to the rest of the world.

Health Insurance Portability and Accountability Act

The Health Insurance Portability and Accountability Act (HIPAA) is a US federal law that regulates patient Protected Health Information (PHI).
Azure offers customers a HIPAA Business Associate Agreement (BAA), which stipulates adherence to certain security and privacy provisions in HIPAA and the HITECH Act. To assist customers in their individual compliance efforts, Microsoft offers a BAA to Azure customers as a contract addendum.

International Organization of Standards/International Electrotechnical Commission 27018

Microsoft is the first cloud provider to have adopted the ISO/IEC 27018 code of practice, which covers the processing of personal information by cloud service providers.

Multi-Tier Cloud Security Singapore

After rigorous assessments conducted by the Multi-Tier Cloud Security (MTCS) Certification Body, Microsoft cloud services received MTCS 584:2013 Certification across all three service classifications:

- Infrastructure as a service (IaaS)
- Platform as a service (PaaS)
- Software as a service (SaaS)

Microsoft is the first global cloud solution provider to receive this certification across all three classifications.

Service Organization Controls 1, 2, and 3

Microsoft-covered cloud services are audited at least annually against the Service Organization Controls (SOC) report framework by independent third-party auditors.
The Microsoft cloud services audit covers controls for data security, availability, processing integrity, and confidentiality as applicable to in-scope trust principles for each service.

National Institute of Standards and Technology Cybersecurity Framework

National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) is a voluntary framework that consists of standards, guidelines, and best practices to manage cybersecurity-related risks.
Microsoft cloud services have undergone independent, third-party Federal Risk and Authorization Management Program (FedRAMP) Moderate and High Baseline audits. Microsoft cloud services certified according to the FedRAMP standards.
Additionally, through a validated assessment performed by the Health Information Trust Alliance (HITRUST), a leading security and privacy standards development and accreditation organization, Office 365 is certified to the objectives specified in the NIST CSF.

United Kingdom Government G-Cloud

The United Kingdom (UK) Government G-Cloud is a cloud computing certification for services used by government entities in the United Kingdom. Azure has received official accreditation from the UK government.

From <https://docs.microsoft.com/en-us/learn/modules/examine-privacy-compliance-data-protection-standards/2-explore-compliance-terms-requirements>

Access the Microsoft Privacy Statement, the Online Services Terms, and the Data Protection Addendum

- 3 minutes

In this part, you learn how the Microsoft Privacy Statement, the Online Services Terms, and the Data Protection Addendum explain what personal data Microsoft collects, how Microsoft uses it, and for what purposes.
For Tailwind Traders, understanding Microsoft's commitment to privacy helps ensure that their customer and application data will be protected.
Let's begin with a brief look at the Microsoft Privacy Statement.

What's in the Microsoft Privacy Statement?

The Microsoft Privacy Statement explains what personal data Microsoft collects, how Microsoft uses it, and for what purposes.
The privacy statement covers all of Microsoft's services, websites, apps, software, servers, and devices. This list ranges from enterprise and server products to devices that you use in your home to software that students use at school.
Microsoft's privacy statement also provides information that's relevant to specific products such as Windows and Xbox.

What's in the Online Services Terms?

The Online Services Terms (OST) is a legal agreement between Microsoft and the customer. The OST details the obligations by both parties with respect to the processing and security of customer data and personal data. The OST applies specifically to Microsoft's online services that you license through a subscription, including Azure, Dynamics 365, Office 365, and Bing Maps.

What is the Data Protection Addendum?

The Data Protection Addendum (DPA) further defines the data processing and security terms for online services. These terms include:

- Compliance with laws.
- Disclosure of processed data.
- Data Security, which includes security practices and policies, data encryption, data access, customer responsibilities, and compliance with auditing.
- Data transfer, retention, and deletion.

To access the DPA:

1. Go to the Licensing Terms and Documentation .
2. In the search bar, enter DPA.
3. From the search results, locate the link to the DPA in your preferred language.
   Alternatively, in the search bar that appears, enter your preferred language to filter the results. Here's an example that retrieves the English version of the DPA.

Search for Documents:
DPA

Note: This page does not include any signed Volume Licensing agreements, enrollments or Microsoft Business and Services Agreement, and is intended solely for reference purposes.

Show Archived

Search: English

Title	Language	Sectors	Regions
MicrosoftOnlineServicesDPA(WW)(English)(July212020)	English	Commercial, Public Sector, Third Party, Common Document, Academic, Government, Nonprofit	North America, EU-EFTA (European Union and EFTA), MEA-EE (Middle East, Africa - Eastern Europe, Asia , WW (World

Transparency is important when it comes to how a cloud provider communicates its privacy policies and how it treats your data. The Microsoft Privacy Statement, the OST, and the DPA detail Microsoft's commitment to protecting data and privacy in the cloud.

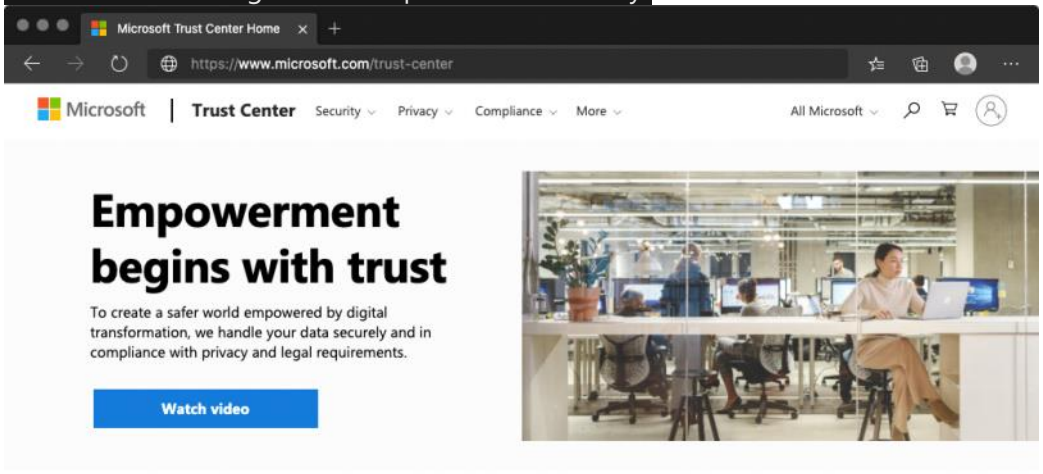
From <https://docs.microsoft.com/en-us/learn/modules/examine-privacy-compliance-data-protection-standards/3-access-microsoft-privacy-statement>

Explore the Trust Center

- 3 minutes

Tailwind Traders needs to stay up to date on the latest security standards for protecting its data. Today, the security team needs to verify whether Azure meets ISO 27001, a commonly used information security standard. Where can the company access this information?

The Trust Center showcases Microsoft's principles for maintaining data integrity in the cloud and how Microsoft implements and supports security, privacy, compliance, and transparency in all Microsoft cloud products and services. The Trust Center is an important part of the Microsoft Trusted Cloud Initiative and provides support and resources for the legal and compliance community.



The Trust Center provides:

- In-depth information about security, privacy, compliance offerings, policies, features, and practices across

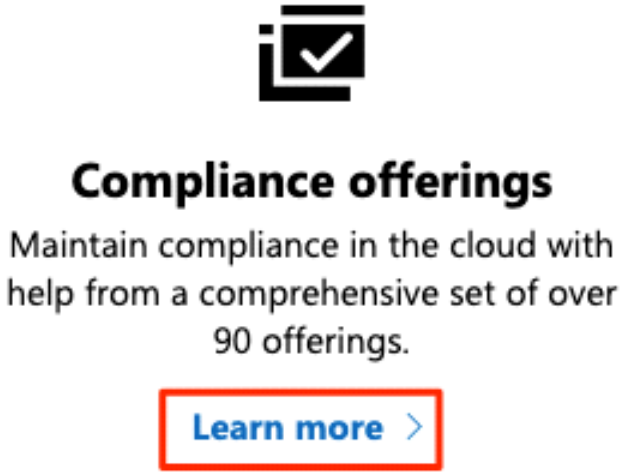
Microsoft cloud products.
- Additional resources for each topic.
- Links to the security, privacy, and compliance blogs and upcoming events.

The Trust Center is a great resource for other people in your organization who might play a role in security, privacy, and compliance. These people include business managers, risk assessment and privacy officers, and legal compliance teams.

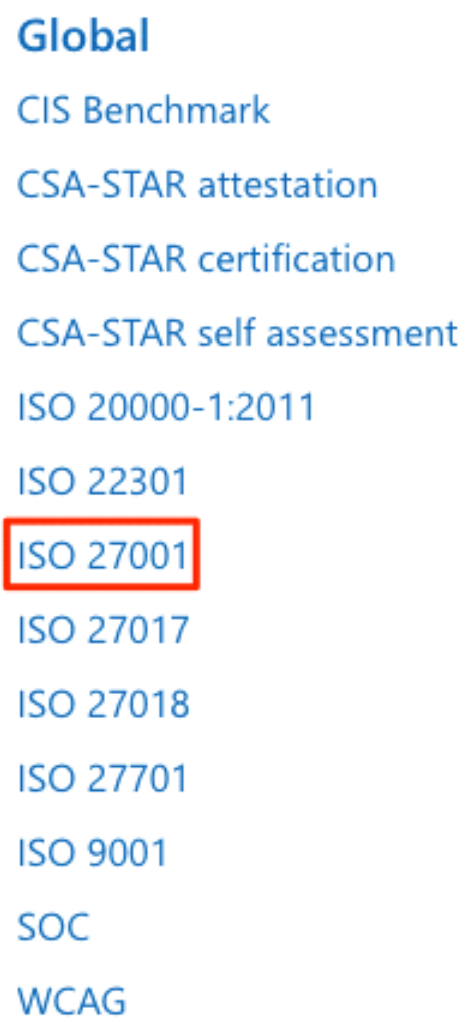
Explore the Trust Center

As an optional exercise, let's take a brief look at the Trust Center's entry for ISO 27001.
Access to the Trust Center doesn't require an Azure subscription or a Microsoft account.

1. Go to the Trust Center.
2. Locate the Additional resources section on the page. Under Compliance offerings, select Learn more.



   You're taken to Microsoft compliance offerings.
   The offerings are grouped into four categories: Global, US Government, Industry, and Regional.
3. Under Global, select ISO 27001.



The ISO 27001 Information Security Management Standards page is typical of the type of compliance information we provide.

4. Briefly review the documentation for ISO/IEC 27001.
   You see:
   - An overview of the standard.
   - Which cloud services are in scope.
   - An overview of the audit cycle and links to audit reports.
   - Answers to frequently asked questions.
   - Additional resources and white papers.

   The areas of documentation for other compliance offerings will vary, but this format is the typical one that you'll find.

From <https://docs.microsoft.com/en-us/learn/modules/examine-privacy-compliance-data-protection-standards/4-explore-trust-center>

Access Azure compliance documentation

- 4 minutes

Here, you learn how to access detailed documentation about legal and regulatory standards and compliance on Azure.

E-commerce is an important part of Tailwind Traders' sales strategy. Its online retail store enables customers to easily browse and order products. Customers typically pay by credit card, so Tailwind Traders has a responsibility

under the Payment Card Industry (PCI) Data Security Standard (DSS). This global standard, known as PCI DSS, seeks to prevent fraud through increased control of credit card data. The standard applies to any organization that stores, processes, or transmits payment and cardholder data.

You've been tasked with investigating whether hosting the company's e-commerce application on Azure would be compliant with PCI DSS. You start with the Azure compliance documentation.

What is the Azure compliance documentation?

The Azure compliance documentation provides you with detailed documentation about legal and regulatory standards and compliance on Azure.

Here you find compliance offerings across these categories:

- Global
- US government
- Financial services
- Health
- Media and manufacturing
- Regional

There are also additional compliance resources, such as audit reports, privacy information, compliance implementations and mappings, and white papers and analyst reports. Country and region privacy and compliance guidelines are also included. Some resources might require you to be signed in to your cloud service to access them.

Examine PCI DSS compliance

The legal team at Tailwind Traders wants to learn more about how PCI DSS relates to the company's e-commerce application on Azure.

As an optional exercise, here you follow along.

1. Go to the Azure compliance documentation .
2. Under Financial services, select PCI DSS.

There you see:

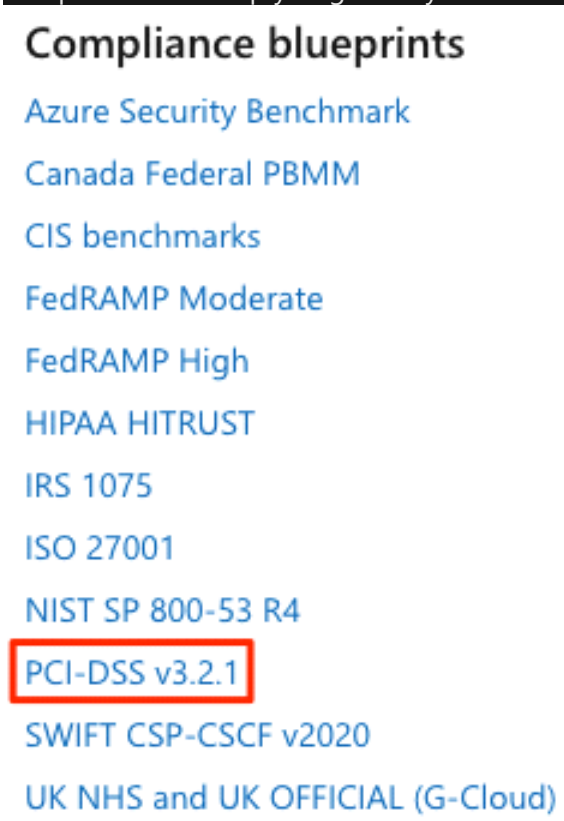
- An overview of the PCI DSS standard.
- How PCI DSS applies to Microsoft.
- Which cloud services are in scope.
- An overview of the audit cycle.
- Answers to frequently asked questions.
- Additional resources and white papers.

Access additional compliance resources

From the Azure compliance documentation , you can access additional compliance resources. For example, from the Audit reports section, you find a link to audit reports for PCI DSS .

From there, you can access several different files, including the Attestation of Compliance reports and the PCI DSS Shared Responsibility Matrix.

Under Compliance blueprints, you find reference blueprints, or policy definitions, for common standards that you can apply to your Azure subscription. The PCI DSS blueprint deploys a core set of policies that map to PCI DSS compliance and help you govern your Azure workloads against this standard.



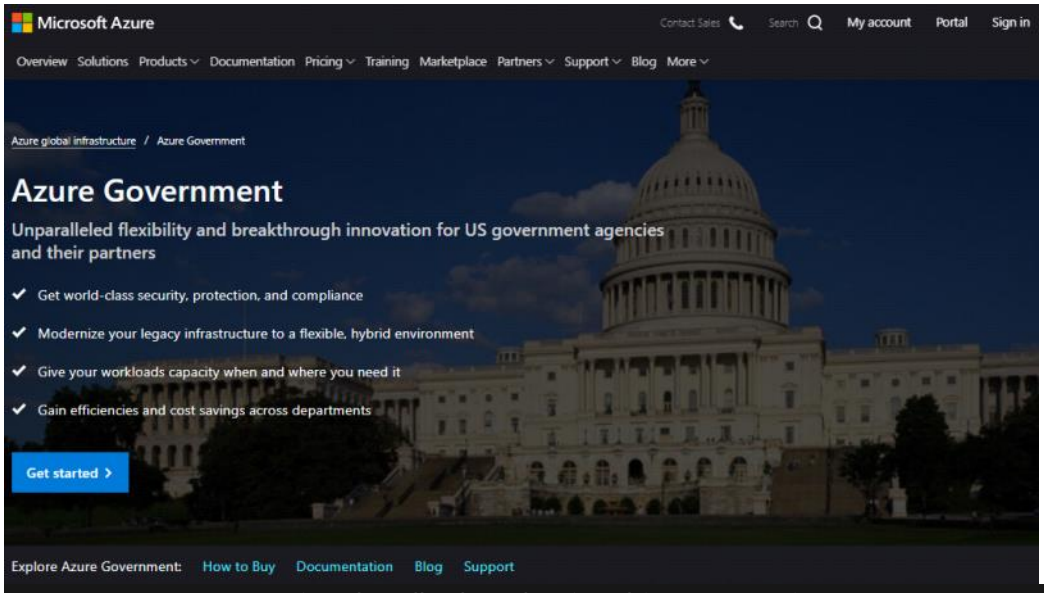
You can then see if the Azure resources in your application architecture have been configured correctly for PCI DSS compliance, or which resources you need to remediate.
Because standards evolve, the Tailwind Traders team might check the audit report periodically to ensure that Azure has any recent changes.

From <https://docs.microsoft.com/en-us/learn/modules/examine-privacy-compliance-data-protection-standards/5-access-azure-compliance-documentation>

What is Azure Government?

- 2 minutes

Azure Government is a separate instance of the Microsoft Azure service. It addresses the security and compliance needs of US federal agencies, state and local governments, and their solution providers. Azure Government offers physical isolation from non-US government deployments and provides screened US personnel.



Azure Government services handle data that is subject to certain government regulations and requirements:

- Federal Risk and Authorization Management Program (FedRAMP)
- National Institute of Standards and Technology (NIST) 800.171 Defense Industrial Base (DIB)
- International Traffic in Arms Regulations (ITAR)
- Internal Revenue Service (IRS) 1075
- Department of Defense (DoD) L4
- Criminal Justice Information Service (CJIS)

To provide the highest level of security and compliance, Azure Government uses physically isolated datacenters and networks located only in the US. Azure Government customers, such as the US federal, state, and local government or their partners, are subject to validation of eligibility.

Azure Government provides the broadest compliance and Level 5 DoD approval. Azure Government is available in eight geographies and offers the most compliance certifications of any cloud provider.

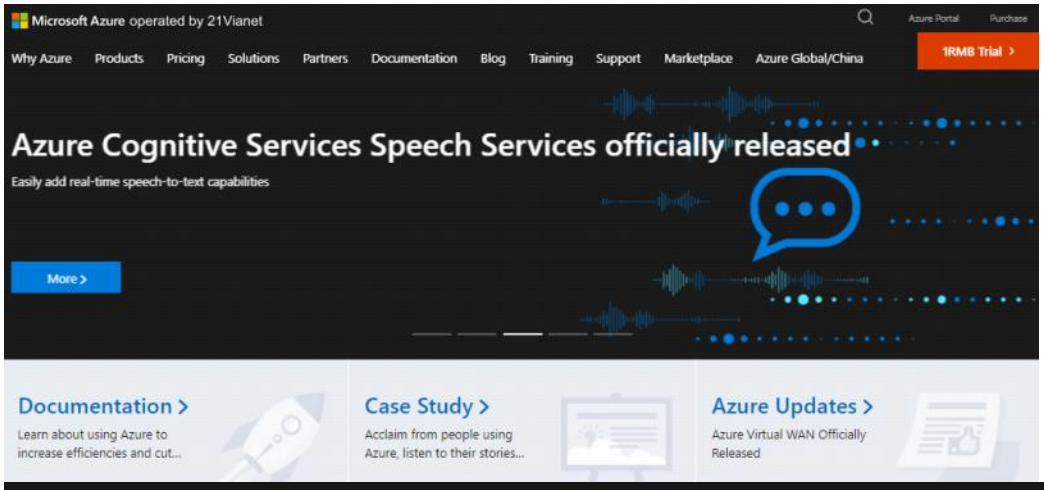
From <https://docs.microsoft.com/en-us/learn/modules/examine-privacy-compliance-data-protection-standards/6-what-is-azure-government>

What is Azure China 21Vianet?

- 2 minutes

Azure China 21Vianet is operated by 21Vianet. It's a physically separated instance of cloud services located in China. Azure China 21Vianet is independently operated and transacted by Shanghai Blue Cloud Technology Co., Ltd. ("21Vianet"), a wholly owned subsidiary of Beijing 21Vianet Broadband Data Center Co., Ltd.

According to the China Telecommunication Regulation, providers of cloud services, infrastructure as a service (IaaS) and platform as a service (PaaS), must have value-added telecom permits. Only locally registered companies with less than 50 percent foreign investment qualify for these permits. To comply with this regulation, the Azure service in China is operated by 21Vianet, based on the technologies licensed from Microsoft.



As the first foreign public cloud service provider offered in China in compliance with government regulations, Azure China 21Vianet provides world-class security as discussed on the Trust Center , as required by Chinese regulations for all systems and applications built on its architecture.

Azure products and services available in China

The Azure services are based on the same Azure, Office 365, and Power BI technologies that make up the Microsoft global cloud service, with comparable service levels. Azure agreements and contracts in China, where applicable, are signed between customers and 21Vianet.
Azure includes the core components of IaaS, PaaS, and software as a service (SaaS). These components include network, storage, data management, identity management, and many other services.
Azure China 21Vianet supports most of the same services that global Azure has, such as geosynchronous data replication and autoscaling. Even if you already use global Azure services, to operate in China you might need to rehost or refactor some or all your applications or services.

From <https://docs.microsoft.com/en-us/learn/modules/examine-privacy-compliance-data-protection-standards/7-what-is-azure-china-21vianet>

Part 6: Describe Azure cost management and service level agreements

Thursday, January 28, 2021 10:57 AM

Plan and manage your Azure costs

Thursday, January 28, 2021 10:57 AM

Learn about the factors that influence cost and tools you can use to help estimate and manage your cloud spend.

Overview

- Introduction 3 min
- Compare costs by using the Total Cost of Ownership Calculator 5 min
- Exercise - Compare sample workload costs by using the TCO Calculator 6 min
- Purchase Azure services 8 min
- Exercise - Estimate workload cost by using the Pricing calculator 6 min
- Manage and minimize total cost on Azure 11 min
- Knowledge check 2 min
- Summary 2 min

From <https://docs.microsoft.com/en-us/learn/paths/az-900-describe-azure-cost-management-service-level-agreements/>

Introduction

- 3 minutes

In this module, you'll learn about the major factors that influence the cost of running in the cloud. Along the way, you'll get hands-on experience with some of the tools you can use to estimate the costs of running your workloads on Azure to help ensure that you stay within budget and use only the services that you need.

Meet Tailwind Traders

Tailwind Traders is a fictitious home improvement retailer. It operates retail hardware stores across the globe and online.

Tailwind Traders specializes in competitive pricing, fast shipping, and a large range of items. It's looking at cloud technologies to improve business operations and support growth into new markets. By moving to the cloud, the company plans to enhance its shopping experience to further differentiate itself from competitors.

How will Tailwind Traders manage cloud costs?

Tailwind Traders is planning its migration to the cloud. The company has run a few successful proof-of-concept projects and wants to better understand how to manage its costs before it moves its workloads to Azure.

Running in the datacenter requires you to maintain a facility and purchase, power, cool, and maintain your servers. Running in the cloud presents new ways to think about your IT expenses.

To answer the question of how much it will cost, you need to understand the factors that influence cost. You also need to understand what tools are available to you to help estimate and manage your cloud spend.

Learning objectives

After completing this module, you'll be able to:

- Use the Total Cost of Ownership Calculator to compare your current datacenter costs to running the same workloads on Azure.
- Describe the different ways you can purchase Azure products and services.
- Use the Pricing calculator to estimate the monthly cost of running your cloud workloads.
- Define some of the major factors that affect total cost, and apply recommended practices to minimize cost.

Prerequisites

- You should be familiar with basic computing concepts and terminology.
- Familiarity with cloud computing is helpful but isn't necessary.

From <https://docs.microsoft.com/en-us/learn/modules/plan-manage-azure-costs/1-introduction>

Compare costs by using the Total Cost of Ownership Calculator

- 5 minutes

Before Tailwind Traders takes its next steps toward migrating to the cloud, it wants to better understand what it spends today in its datacenter.

Having a firm understanding of where the company is today will give it a greater sense of what cloud migration means in terms of cost.

In this unit, you'll see how the Total Cost of Ownership (TCO) Calculator can help you compare the cost of running in the datacenter versus running on Azure.

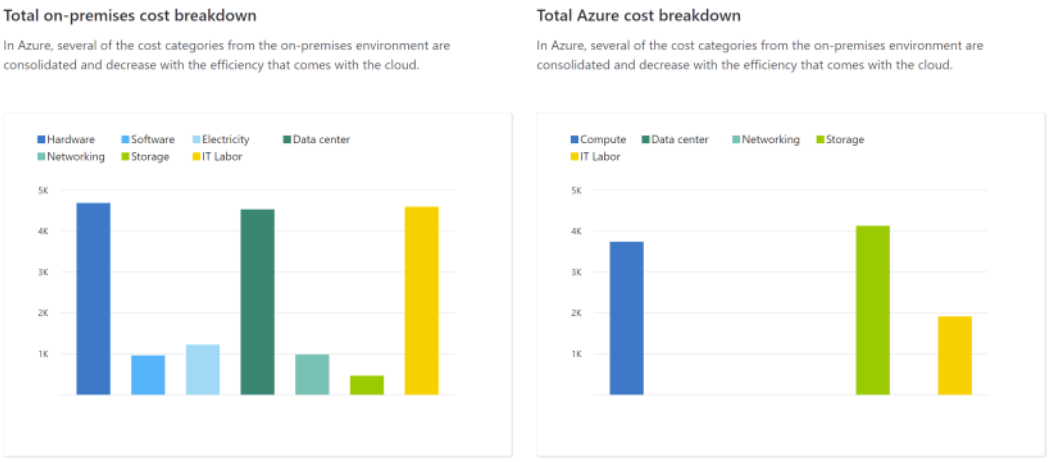
What's the TCO Calculator?

The TCO Calculator helps you estimate the cost savings of operating your solution on Azure over time, instead of in your on-premises datacenter.

The term *total cost of ownership* is commonly used in finance. It can be hard to see all the hidden costs related to operating a technology capability on-premises. Software licenses and hardware are additional costs.

With the TCO Calculator, you enter the details of your on-premises workloads. Then you review the suggested industry average cost (which you can adjust) for related operational costs. These costs include electricity, network maintenance, and IT labor. You're then presented with a side-by-side report. Using the report, you can compare those costs with the same workloads running on Azure.

The following image shows one example.



Note

You don't need an Azure subscription to work with the TCO Calculator.

How does the TCO Calculator work?

Working with the TCO Calculator involves three steps:

- Define your workloads.
- Adjust assumptions.
- View the report.

Let's take a closer look at each step.

Step 1: Define your workloads

First, you enter the specifications of your on-premises infrastructure into the TCO Calculator, based on these four categories:

- Servers
  This category includes operating systems, virtualization methods, CPU cores, and memory (RAM).
- Databases
  This category includes database types, server hardware, and the Azure service you want to use, which includes the expected maximum concurrent user sign-ins.
- Storage
  This category includes storage type and capacity, which includes any backup or archive storage.
- Networking
  This category includes the amount of network bandwidth you currently consume in your on-premises environment.

Step 2: Adjust assumptions

Next, you specify whether your current on-premises licenses are enrolled for Software Assurance , which can

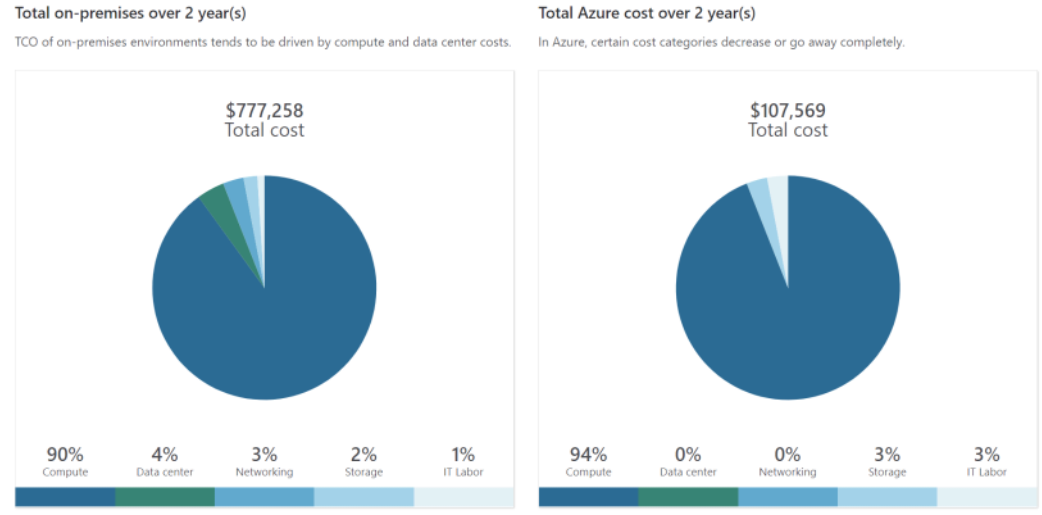
save you money by reusing those licenses on Azure. You also specify whether you need to replicate your storage to another Azure region for greater redundancy.
Then, you can see the key operating cost assumptions across several different areas, which vary among teams and organizations. These costs have been certified by Nucleus Research, an independent research company. For example, these costs include:

- Electricity price per kilowatt hour (KWh).
- Hourly pay rate for IT administration.
- Network maintenance cost as a percentage of network hardware and software costs.

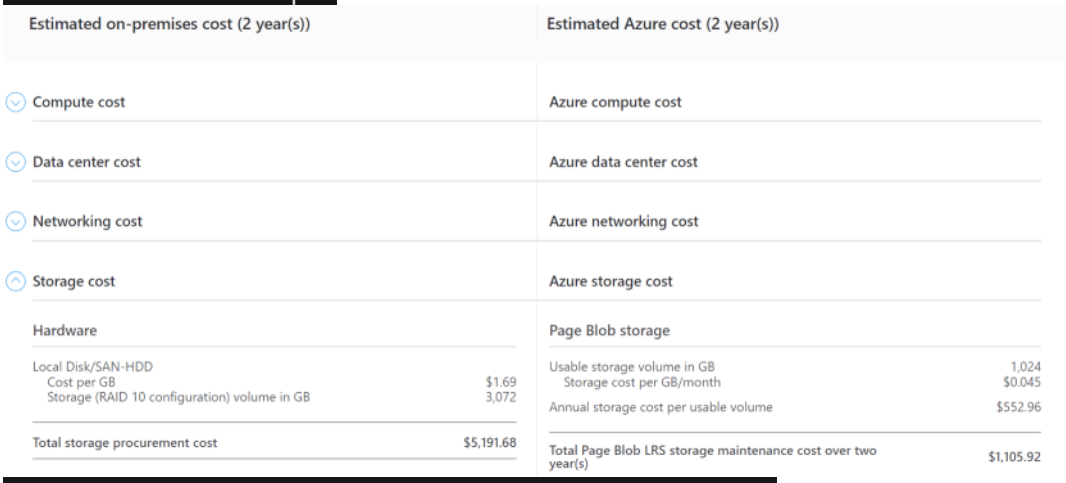
To improve the accuracy of the TCO Calculator results, you adjust the values so that they match the costs of your current on-premises infrastructure.

Step 3: View the report

Choose a time frame between one and five years. the TCO Calculator generates a report that's based on the information you've entered. Here's an example:



For each category (compute, datacenter, networking, storage, and IT labor), you can also view a side-by-side comparison of the cost breakdown of operating those workloads on-premises versus operating them on Azure. Here's an example:



You can download, share, or save this report to review later.
In the next unit, you'll use the TCO Calculator to help the Tailwind Traders team understand their total costs.

From <https://docs.microsoft.com/en-us/learn/modules/plan-manage-azure-costs/2-compare-costs-tco-calculator>

Exercise - Compare sample workload costs by using the TCO Calculator

- 6 minutes

In this exercise, you use the Total Cost of Ownership (TCO) Calculator to compare the cost of running a sample workload in the datacenter versus on Azure.

Tailwind Traders is interested in moving some of its on-premises workloads to the cloud. But first, the Chief Financial Officer wants to understand more about moving from a relatively fixed cost structure to an ongoing monthly cost structure.

You've been tasked to investigate whether there are any potential cost savings in moving your European datacenter to the cloud over the next three years. You need to take into account all of the potentially hidden costs involved with operating on-premises and in the cloud.

Instead of manually collecting everything you think might be included, you use the TCO Calculator as a starting point. You adjust the provided cost assumptions to match Tailwind Traders' on-premises environment.

Note

Remember, you don't need an Azure subscription to work with the TCO Calculator.

Let's say that:

- Tailwind Traders runs two sets, or banks, of 50 virtual machines (VMs) in each bank.
- The first bank of VMs runs Windows Server under Hyper-V virtualization.
- The second bank of VMs runs Linux under VMware virtualization.
- There's also a storage area network (SAN) with 60 terabytes (TB) of disk storage.
- You consume an estimated 15 TB of outbound network bandwidth each month.
- There are also a number of databases involved, but for now, you'll omit those details.

Recall that the TCO Calculator involves three steps:

Let's see how Tailwind Traders' existing workloads compare in the datacenter versus on Azure.

Define your workloads

Enter the specifications of your on-premises infrastructure into the TCO Calculator.

1. Go to the TCO Calculator .
2. Under Define your workloads, select Add server workload to create a row for your bank of Windows Server VMs.
3. Under Servers, set the value for each of these settings:

Setting	Value
Name	Servers: Windows VMs
Workload	Windows/Linux Server
Environment	Virtual Machines
Operating system	Windows
VMs	50
Virtualization	Hyper-V

Core(s)	8
RAM (GB)	16
Optimize by	CPU
Windows Server 2008/2008 R2	Off

TABLE 1

4. Select Add server workload to create a second row for your bank of Linux VMs. Then specify these settings:

Setting	Value
Name	Servers: Linux VMs
Workload	Windows/Linux Server
Environment	Virtual Machines
Operating system	Linux
VMs	50
Virtualization	VMware
Core(s)	8
RAM (GB)	16
Optimize by	CPU

TABLE 2

5. Under Storage, select Add storage. Then specify these settings:

Setting	Value
Name	Server Storage
Storage type	Local Disk/SAN
Disk type	HDD
Capacity	60 TB
Backup	120 TB
Archive	0 TB

TABLE 3

6. Under Networking, set Outbound bandwidth to 15 TB.
7. Select Next.

Adjust assumptions

Here, you specify your currency. For brevity, you leave the remaining fields at their default values.
In practice, you would adjust any cost assumptions and make any adjustments to match your current on-premises environment.

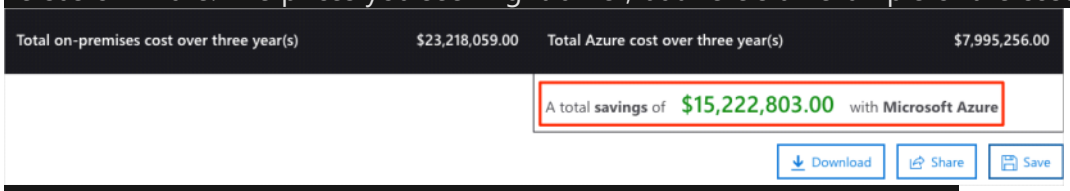
1. At the top of the page, select your currency. This example uses US Dollar ($).
2. Select Next.

View the report

Take a moment to review the generated report.
Remember, you've been tasked to investigate cost savings for your European datacenter over the next three years.
To make these adjustments:

1. Set Timeframe to 3 Years.
2. Set Region to North Europe.

Scroll to the summary at the bottom. You see a comparison of running your workloads in the datacenter versus on Azure. The prices you see might differ, but here's an example of the cost savings you might expect.



Select Download to download or print a copy of the report in PDF format.

Great work. You now have the information that you can share with your Chief Financial Officer. If you need to make adjustments, you can revisit the TCO Calculator to generate a fresh report.

From <https://docs.microsoft.com/en-us/learn/modules/plan-manage-azure-costs/3-compare-workload-costs-tco-calculator>

Purchase Azure services

- 8 minutes

In this unit, you learn how to purchase Azure services and get a sense for other factors that affect cost.

You meet with your Chief Financial Officer and some of the team leads. You learn about some assumptions you've missed. You were able to quickly update your total estimated spend through the Total Cost of Ownership (TCO) Calculator.

During the meeting, some new questions arose as the discussion moves toward cloud migration:

- What types of Azure subscriptions are available?
- How do we purchase Azure services?
- Does location or network traffic affect cost?
- What other factors affect the final cost?
- How can we get a more detailed estimate of the cost to run on Azure?

It's important to learn how costs are generated in Azure so that you can understand how your purchasing and solution design decisions can impact your final cost. You agree to research these questions, so let's review each one in greater detail.

What types of Azure subscriptions can I use?

You probably know that an Azure *subscription* provides you with access to Azure resources, such as virtual machines (VMs), storage, and databases. The types of resources you use impact your monthly bill.

Azure offers both free and paid subscription options to fit your needs and requirements. They are:

- Free trial
  A free trial subscription provides you with 12 months of popular free services, a credit to explore any Azure service for 30 days, and more than 25 services that are always free. Your Azure services are disabled when the trial ends or when your credit expires for paid products, unless you upgrade to a paid subscription.
- Pay-as-you-go
  A pay-as-you-go subscription enables you to pay for what you use by attaching a credit or debit card to your account. Organizations can apply for volume discounts and prepaid invoicing.
- Member offers
  Your existing membership to certain Microsoft products and services might provide you with credits for

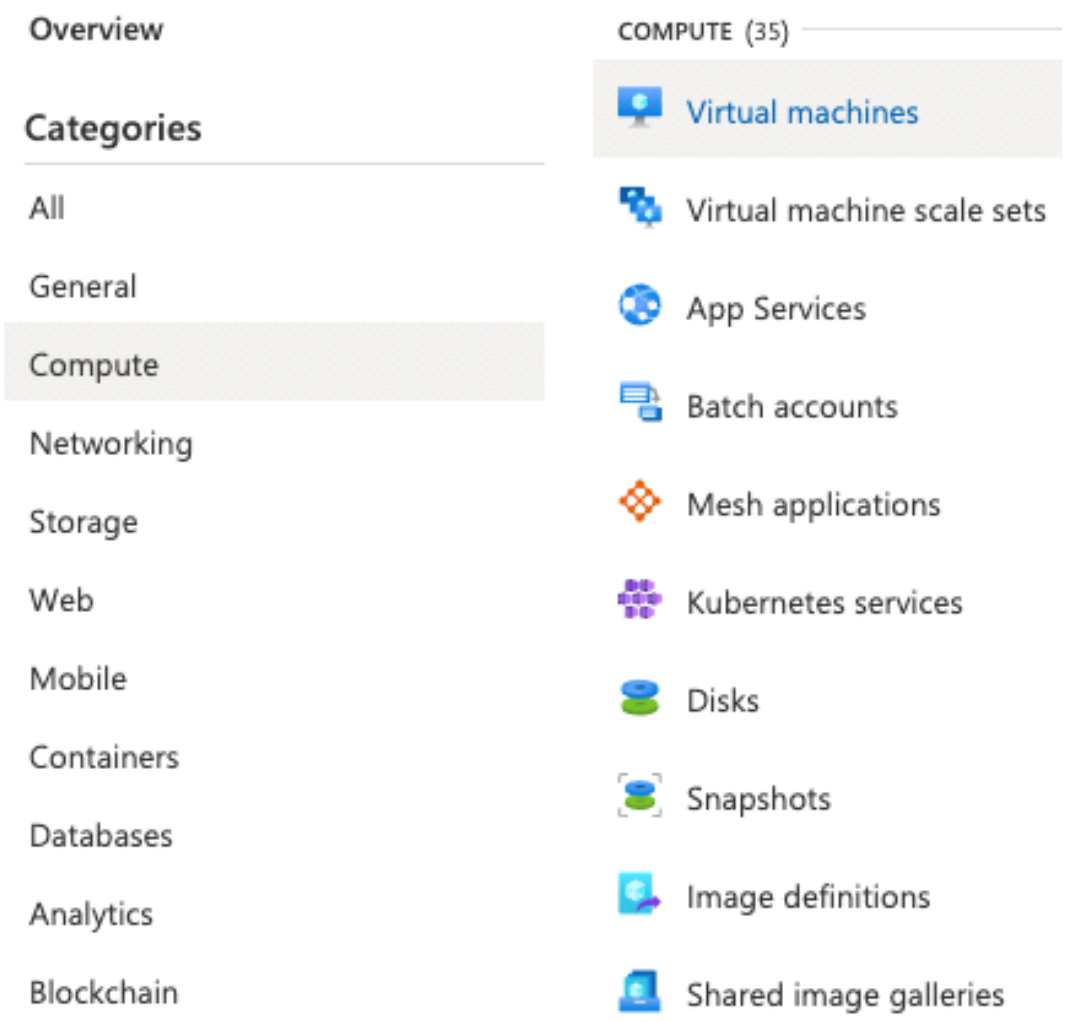
your Azure account and reduced rates on Azure services. For example, member offers are available to Visual Studio subscribers, Microsoft Partner Network members, Microsoft for Startups members, and Microsoft Imagine members.

How do I purchase Azure services?

There are three main ways to purchase services on Azure. They are:

- Through an Enterprise Agreement
  Larger customers, known as enterprise customers, can sign an Enterprise Agreement with Microsoft. This agreement commits them to spending a predetermined amount on Azure services over a period of three years. The service fee is typically paid annually. As an Enterprise Agreement customer, you'll receive the best customized pricing based on the kinds and amounts of services you plan on using.
- Directly from the web
  Here, you purchase Azure services directly from the Azure portal website and pay standard prices. You're billed monthly, as a credit card payment or through an invoice. This purchasing method is known as Web Direct.
- Through a Cloud Solution Provider
  A Cloud Solution Provider (CSP) is a Microsoft Partner who helps you build solutions on top of Azure. Your CSP bills you for your Azure usage at a price they determine. They also answer your support questions and escalate them to Microsoft, as needed.

You can bring up, or *provision*, Azure resources from the Azure portal or from the command line. The Azure portal arranges products and services by category. You select the services that fit your needs. Your account is billed according to Azure's "pay for what you use" model.
Here's an example that shows the Azure portal.



At the end of each month, you're billed for what you've used. At any time, you can check the cost management and billing page in the Azure portal to get a summary of your current usage and review invoices from prior months.

What factors affect cost?

The way you use resources, your subscription type, and pricing from third-party vendors are common factors. Let's take a quick look at each.

Resource type

A number of factors influence the cost of Azure resources. They depend on the type of resource or how you customize it.
For example, with a storage account you specify a type (such as block blob storage or table storage), a performance tier (standard or premium), and an access tier (hot, cool, or archive). These selections present different costs.

Usage meters

When you provision a resource, Azure creates *meters* to track usage of that resource. Azure uses these meters

to generate a usage record that's later used to help calculate your bill.
Think of usage meters similar to how you use electricity or water in your home. You might pay a base price each month for electricity or water service, but your final bill is based on the total amount that you consumed.
Let's look at a single VM as an example. The following kinds of meters are relevant to tracking its usage:

- Overall CPU time.
- Time spent with a public IP address.
- Incoming (ingress) and outgoing (egress) network traffic in and out of the VM.
- Disk size and amount of disk read and disk write operations.

Each meter tracks a specific type of usage. For example, a meter might track bandwidth usage (ingress or egress network traffic in bits per second), number of operations, or its size (storage capacity in bytes).
The usage that a meter tracks correlates to a quantity of billable units. Those units are charged to your account for each billing period. The rate per billable unit depends on the resource type you're using.

Resource usage

In Azure, you're always charged based on what you use. As an example, let's look at how this billing applies to deallocating a VM.
In Azure, you can delete or deallocate a VM. Deleting a VM means that you no longer need it. The VM is removed from your subscription, and then it's prepared for another customer.
Deallocating a VM means that the VM is no longer running. But the associated hard disks and data are still kept in Azure. The VM isn't assigned to a CPU or network in Azure's datacenter, so it doesn't generate the costs associated with compute time or the VM's IP address. Because the disks and data are still stored, and the resource is present in your Azure subscription, you're still billed for disk storage.
Deallocating a VM when you don't plan on using it for some time is just one way to minimize costs. For example, you might deallocate the VMs you use for testing purposes on weekends when your testing team isn't using them. You'll learn more about ways to minimize cost later in this module.

Azure subscription types

Some Azure subscription types also include usage allowances, which affect costs.
For example, an Azure free trial subscription provides access to a number of Azure products that are free for 12 months. It also includes credit to spend within your first 30 days of sign-up. And you get access to more than 25 products that are always free (based on resource and region availability).

Azure Marketplace

You can also purchase Azure-based solutions and services from third-party vendors through Azure Marketplace. Examples include managed network firewall appliances or connectors to third-party backup services. Billing structures are set by the vendor.

Does location or network traffic affect cost?

When you provision a resource in Azure, you need to define the location (known as the Azure region) of where it will be deployed. Let's see why this decision can have cost consequences.

Location

Azure infrastructure is distributed globally, which enables you to deploy your services centrally or provision your services closest to where your customers use them.
Different regions can have different associated prices. Because geographic regions can impact where your network traffic flows, network traffic is a cost influence to consider as well.
For example, say Tailwind Traders decides to provision its Azure resources in the Azure regions that offer the lowest prices. That decision would save the company some money. But, if they need to transfer data between those regions, or if their users are located in different parts of the world, any potential savings could be offset by the additional network usage costs of transferring data between those resources.

Zones for billing of network traffic

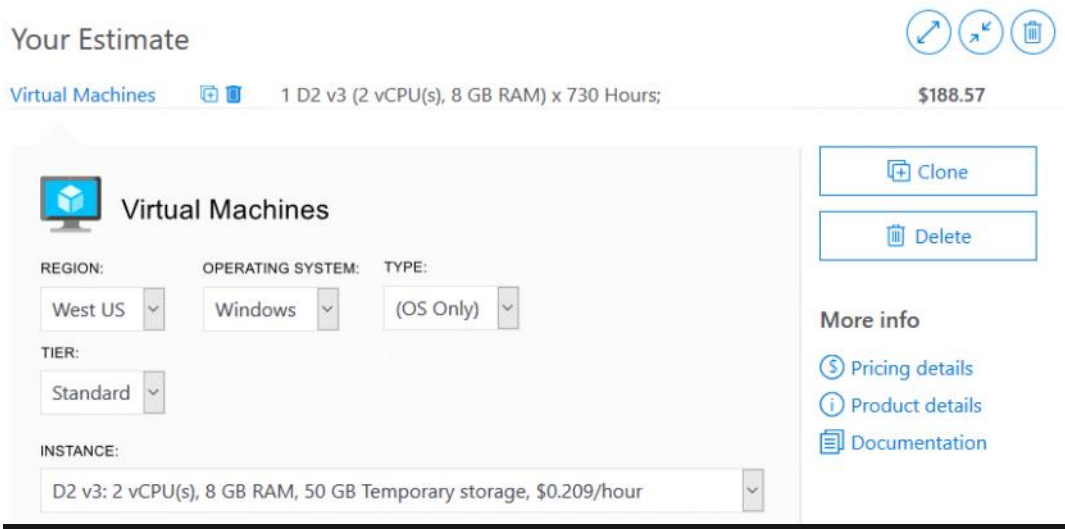
Billing zones are a factor in determining the cost of some Azure services.
Bandwidth refers to data moving in and out of Azure datacenters. Some inbound data transfers (data going into Azure datacenters) are free. For outbound data transfers (data leaving Azure datacenters), data transfer pricing is based on *zones*.

A zone is a geographical grouping of Azure regions for billing purposes. The following zones include some of the regions as shown here:

- Zone 1: Australia Central, West US, East US, Canada West, West Europe, France Central, and others
- Zone 2: Australia East, Japan West, Central India, Korea South, and others
- Zone 3: Brazil South, South Africa North, South Africa West, UAE Central, UAE North
- DE Zone 1: Germany Central, Germany Northeast

How can I estimate the total cost?

As you've learned, an accurate cost estimate takes all of the preceding factors into account. Fortunately, the Azure Pricing calculator helps you with that process.
The Pricing calculator displays Azure products in categories. You add these categories to your estimate and configure according to your specific requirements. You then receive a consolidated estimated price, with a detailed breakdown of the costs associated with each resource you added to your solution. You can export or share that estimate or save it for later. You can load a saved estimate and modify it to match updated requirements.
You also can access pricing details, product details, and documentation for each product from within the Pricing calculator.



The options that you can configure in the Pricing calculator vary between products, but they can include:

- Region
  A region is the geographical location in which you can provision a service. Southeast Asia, Central Canada, Western United States, and Northern Europe are a few examples.
- Tier
  Tiers, such as the Free tier or Basic tier, have different levels of availability or performance and different associated costs.
- Billing options
  Billing options highlight the different ways you can pay for a service. Options can vary based on your customer type and subscription type and can include options to save costs.
- Support options
  These options enable you to select additional support pricing options for certain services.
- Programs and offers
  Your customer or subscription type might enable you to choose from specific licensing programs or other offers.
- Azure Dev/Test pricing
  This option lists the available prices for development and test workloads. Dev/Test pricing applies when you run resources within an Azure subscription that's based on a Dev/Test offer.

Keep in mind that the Pricing calculator provides estimates and *not* actual price quotes. Actual prices can vary depending upon the date of purchase, the payment currency you're using, and the type of Azure customer you are.

From <https://docs.microsoft.com/en-us/learn/modules/plan-manage-azure-costs/4-purchase-azure-services>

Exercise - Estimate workload cost by using the Pricing calculator

- 6 minutes

In this exercise, you use the Pricing calculator to estimate the cost of running a basic web application on Azure. With an understanding of the more important cost factors associated with running on Azure, Tailwind Traders wants to take a typical workload and estimate how much it would cost each month to run it on Azure.

The IT Manager at Tailwind Traders is faced with the decision about whether to replace some aging on-premises hardware or move the application to Azure. The company needs to know how much the ongoing monthly cost of the solution in Azure would be.

Let's start by defining which Azure services you need.

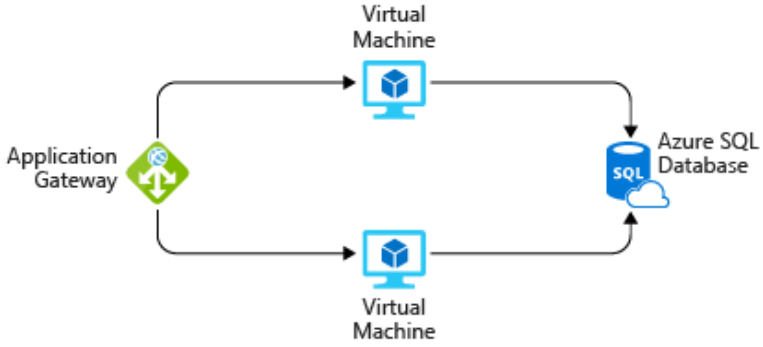
Note
The Pricing calculator is for information purposes only. The prices are only an estimate, and you won't be charged for any services you select.

Define your requirements

Before you run the Pricing calculator, you first need a sense of what Azure services you need.
You meet with the application development team to discuss their migration project.
In their datacenter, the team has an ASP.NET web application that runs on Windows. The web application provides information about product inventory and pricing. They have two virtual machines that are connected through a central load balancer. The web application connects to a SQL Server database that holds inventory and pricing information.
The team decides to:

- Use Azure Virtual Machines instances, similar to the virtual machines they use in the datacenter.
- Use Azure Application Gateway for load balancing.
- Use Azure SQL Database to hold inventory and pricing information.

Here's a diagram that shows the basic configuration:



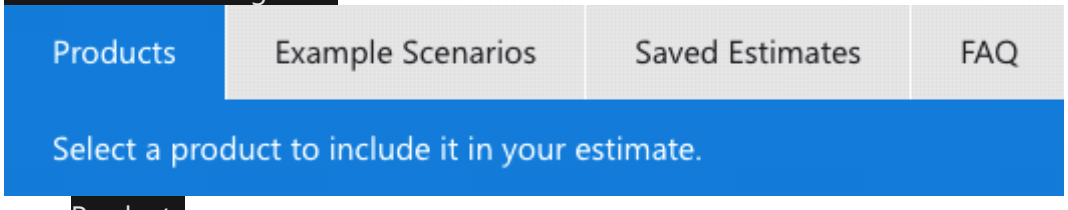
In practice, you would define your requirements in greater detail. But here are some basic facts and requirements that came up during the meeting:

- The application is used by Tailwind Traders employees at their retail stores. It's not accessible to customers.
- This application doesn't require a massive amount of computing power.
- The virtual machines and the database run all the time (730 hours per month).
- The network processes about 1 TB of data per month.
- The database doesn't need to be configured for high-performance workloads and requires no more than 32 GB of storage.

Explore the Pricing calculator

Let's start with a quick tour of the Pricing calculator.

1. Go to the Pricing calculator .
2. Notice the following tabs:



   - Products
     This is where you choose the Azure services that you want to include in your estimate. You'll likely

spend most of your time here.
- Example Scenarios
  Here you'll find several *reference architectures*, or common cloud-based solutions that you can use as a starting point.
- Saved Estimates
  Here you'll find your previously saved estimates.
- FAQ
  Here you'll discover answers to frequently asked questions about the Pricing calculator.

Estimate your solution

Here you add each Azure service that you need to the calculator. Then you configure each service to fit your needs.

Tip

Make sure you have a clean calculator with nothing listed in the estimate. You can reset the estimate by selecting the trash can icon next to each item.

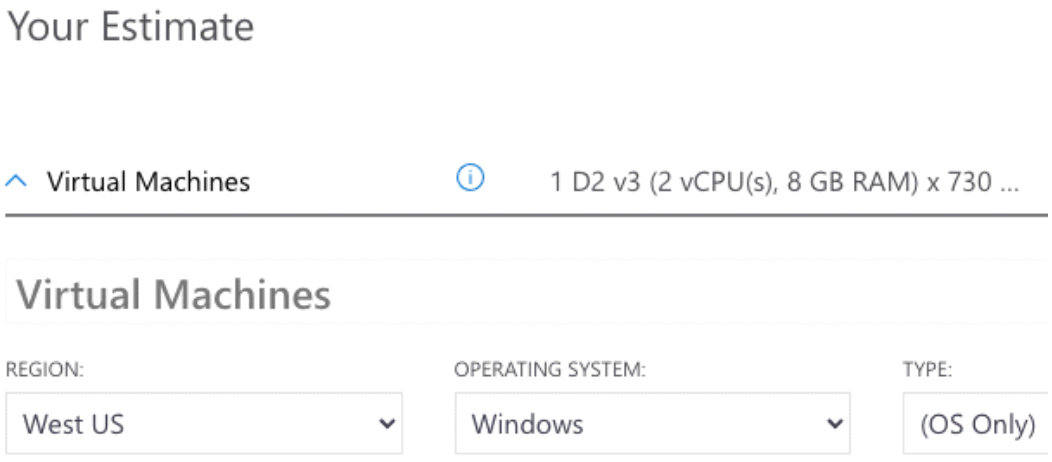
Add services to the estimate

1. On the Products tab, select the service from each of these categories:

Category	Service
Compute	Virtual Machines
Databases	Azure SQL Database
Networking	Application Gateway

TABLE 1

2. Scroll to the bottom of the page. You see that each service is listed with its default configuration.



Configure services to match your requirements

1. Under Virtual Machines, set these values:

Setting	Value
Region	West US
Operating system	Windows

Type	(OS Only)
Tier	Standard
Instance	D2 v3
Virtual machines	2 x 730 Hours

TABLE 2

2. Leave the remaining settings at their current values.
   Under Azure SQL Database, set these values:

Setting	Value
Region	West US
Type	Single Database
Backup storage tier	RA-GRS
Purchase model	vCore
Service tier	General Purpose
Compute tier	Provisioned
Generation	Gen 5
Instance	8 vCore

TABLE 3

3. Leave the remaining settings at their current values.
   Under Application Gateway, set these values:

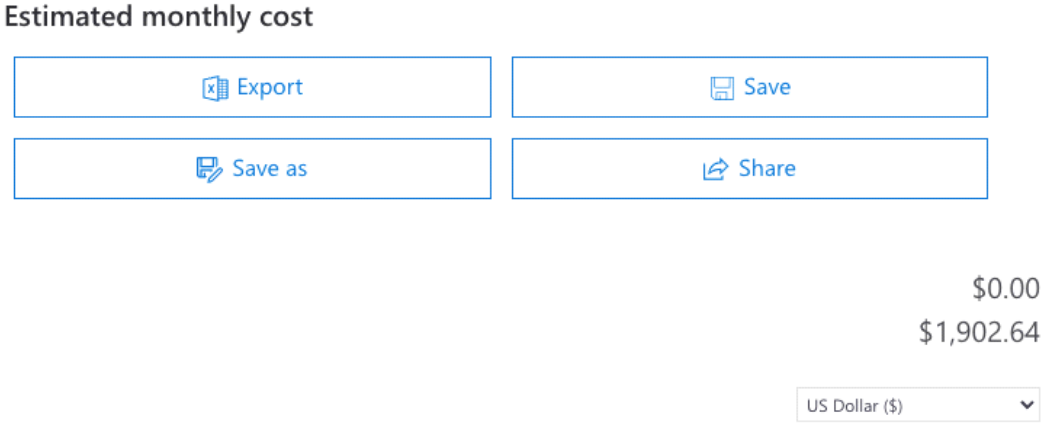
Setting	Value
Region	West US
Tier	Web Application Firewall
Size	Medium
Gateway hours	2 x 730 Hours
Data processed	1 TB
Outbound data transfer	5 GB

TABLE 4

Leave the remaining settings at their current values.

Review, share, and save your estimate

At the bottom of the page, you see the total estimated cost of running the solution. You can change the currency type if you want.



At this point, you have a few options:

- Select Export to save your estimate as an Excel document.
- Select Save or Save as to save your estimate to the Saved Estimates tab for later.
- Select Share to generate a URL so you can share the estimate with your team.

You now have a cost estimate that you can share with your team. You can make adjustments as you discover any changes to your requirements.
Experiment with some of the options you worked with here, or create a purchase plan for a workload you want to run on Azure.

From <https://docs.microsoft.com/en-us/learn/modules/plan-manage-azure-costs/5-estimate-workload-cost-pricing-calculator>

Manage and minimize total cost on Azure

- 11 minutes

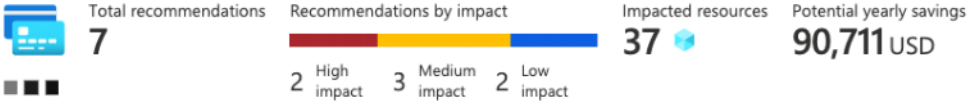
As a home improvement retailer, the proverb "measure twice, cut once" is fitting for the team at Tailwind Traders.
Here are some recommended practices that can help you minimize your costs.

Understand estimated costs before you deploy

To help you plan your solution on Azure, carefully consider the products, services, and resources you need. Read the relevant documentation to understand how each of your choices is metered and billed.
Calculate your projected costs by using the Pricing calculator and the Total Cost of Ownership (TCO) Calculator. Only add the products, services, and resources that you need for your solution.

Use Azure Advisor to monitor your usage

Ideally, you want your provisioned resources to match your actual usage.
Azure Advisor identifies unused or underutilized resources and recommends unused resources that you can remove. This information helps you configure your resources to match your actual workload.
The following image shows some example recommendations from Azure Advisor:



IMPACT	DESCRIPTION	POTENTIAL YEARLY SAVINGS*
High	Right-size or shutdown underutilized virtual machines	82,942.01 USD
High	Buy virtual machine reserved instances to save money over pay-as-you-go costs	538.16 USD
Medium	Right-size underutilized SQL Databases	975.64 USD

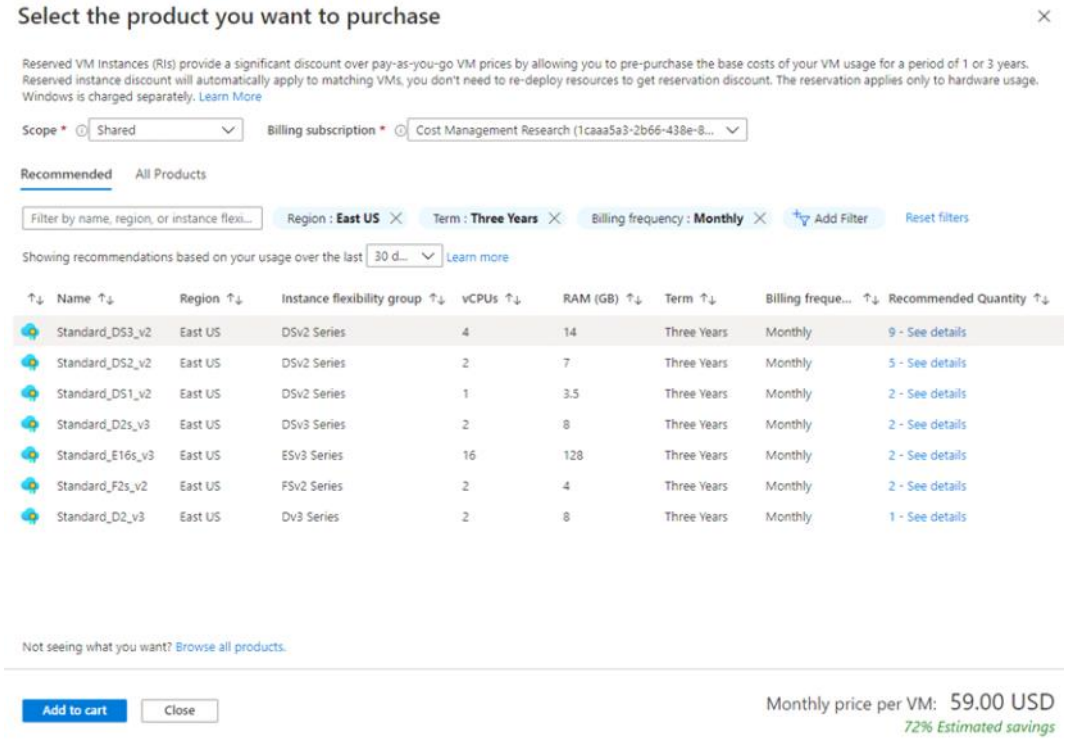
Recommendations are sorted by impact: high, medium, or low. In some cases, Azure Advisor can automatically remediate, or fix, the underlying problem. Other issues, such as the two that are listed as high impact, require human intervention.

Use spending limits to restrict your spending

If you have a free trial or a credit-based Azure subscription, you can use spending limits to prevent accidental overrun.
For example, when you spend all the credit included with your Azure free account, Azure resources that you deployed are removed from production and your Azure virtual machines (VMs) are stopped and deallocated. The data in your storage accounts is available as read-only. At this point, you can upgrade your free trial subscription to a pay-as-you-go subscription.
If you have a credit-based subscription and you reach your configured spending limit, Azure suspends your subscription until a new billing period begins.
A related concept is *quotas*, or limits on the number of similar resources you can provision within your subscription. For example, you can allocate up to 25,000 VMs per region. These limits mainly help Microsoft plan its datacenter capacity.

Use Azure Reservations to prepay

Azure Reservations offers discounted prices on certain Azure services. Azure Reservations can save you up to 72 percent as compared to pay-as-you-go prices. To receive a discount, you reserve services and resources by paying in advance.
For example, you can prepay for one year or three years of use of VMs, database compute capacity, database throughput, and other Azure resources.
The following example shows estimated savings on VMs. In this example, you save an estimated 72 percent by committing to a three-year term.



Azure Reservations are available to customers with an Enterprise Agreement, Cloud Solution Providers, and pay-as-you-go subscriptions.

Choose low-cost locations and regions

The cost of Azure products, services, and resources can vary across locations and regions. If possible, you should use them in those locations and regions where they cost less.

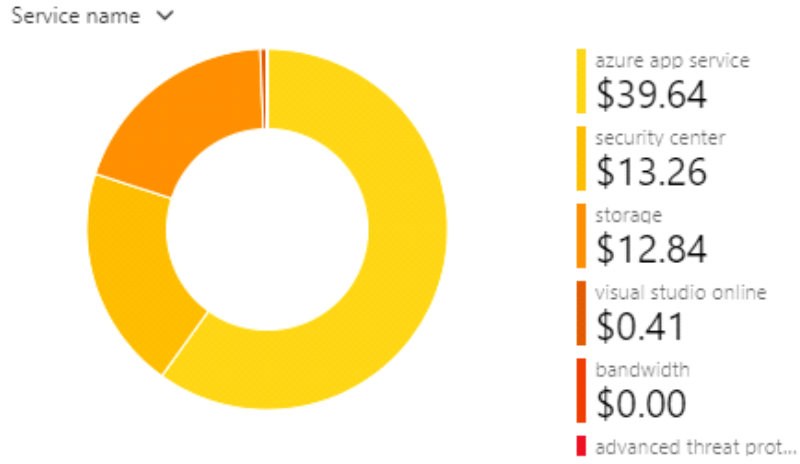
But remember, some resources are metered and billed according to how much outgoing (egress) network bandwidth they consume. You should provision connected resources that are metered by bandwidth in the same Azure region to reduce egress traffic between them.

Research available cost-saving offers

Keep up to date with the latest Azure customer and subscription offers, and switch to offers that provide the greatest cost-saving benefit.

Use Azure Cost Management + Billing to control spending

Azure Cost Management + Billing is a free service that helps you understand your Azure bill, manage your account and subscriptions, monitor and control Azure spending, and optimize resource use.
The following image shows current usage broken down by service:



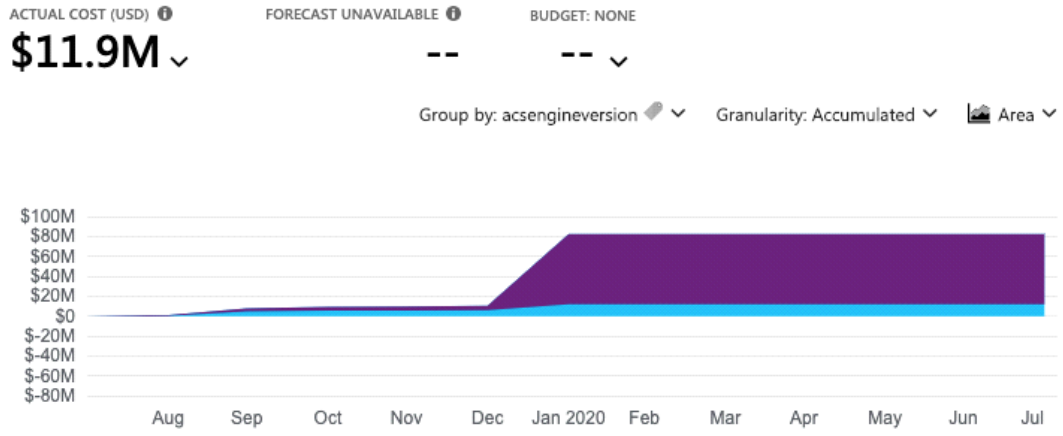
In this example, Azure App Service, a web application hosting service, generates the greatest cost.
Azure Cost Management + Billing features include:

- Reporting
  Use historical data to generate reports and forecast future usage and expenditure.
- Data enrichment
  Improve accountability by categorizing resources with tags that correspond to real-world business and organizational units.
- Budgets
  Create and manage cost and usage budgets by monitoring resource demand trends, consumption rates, and cost patterns.
- Alerting
  Get alerts based on your cost and usage budgets.
- Recommendations
  Receive recommendations to eliminate idle resources and to optimize the Azure resources you provision.

Apply tags to identify cost owners

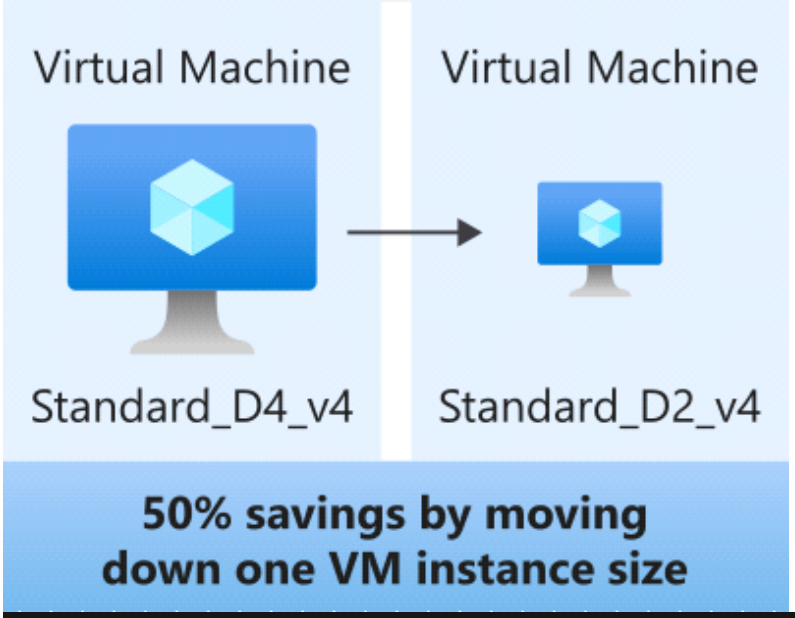
Tags help you manage costs associated with the different groups of Azure products and resources. You can apply tags to groups of Azure resources to organize billing data.
For example, if you run several VMs for different teams, you can use tags to categorize costs by department, such as Human Resources, Marketing, or Finance, or by environment, such as Test or Production.

Tags make it easier to identify groups that generate the biggest Azure costs, which can help you adjust your spending accordingly.
The following image shows a year's worth of usage broken down by tags on the Azure Cost Management + Billing page:



Resize underutilized virtual machines

A common recommendation that you'll find from Azure Cost Management + Billing and Azure Advisor is to resize or shut down VMs that are underutilized or idle.
As an example, say you have a VM whose size is Standard_D4_v4, a general-purpose VM type with four vCPUs and 16 GB of memory. You might discover that this VM is idle 90 percent of the time.
Virtual machine costs are linear and double for each size larger in the same series. So in this case, if you reduce the VM's size from Standard_D4_v4 to Standard_D2_v4, which is the next size lower, you reduce your compute cost by 50 percent.
The following image shows this idea:



Keep in mind that resizing a VM requires it to be stopped, resized, and then restarted. This process might take a few minutes depending on how significant the size change is. Be sure to properly plan for an outage, or shift your traffic to another instance while you perform resize operations.

Deallocate virtual machines during off hours

Recall that to *deallocate* a VM means to no longer run the VM, but preserve the associated hard disks and data in Azure.

If you have VM workloads that are only used during certain periods, but you're running them every hour of every day, you're wasting money. These VMs are great candidates to shut down when not in use and start back when you need them, saving you compute costs while the VM is deallocated.

This approach is an excellent strategy for development and testing environments, where the VMs are needed only during business hours. Azure even provides a way to automatically start and stop your VMs on a schedule.

Delete unused resources

This recommendation might sound obvious, but if you aren't using a resource, you should shut it down. It's not uncommon to find nonproduction or proof-of-concept systems that are no longer needed following the completion of a project.

Regularly review your environment, and work to identify these systems. Shutting down these systems can have a dual benefit by saving you on infrastructure costs and potential savings on licensing and operating costs.

Migrate from IaaS to PaaS services

As you move your workloads to the cloud, a natural evolution is to start with infrastructure as a service (IaaS) services because they map more directly to concepts and operations you're already familiar with.

Over time, one way to reduce costs is to gradually move IaaS workloads to run on platform as a service (PaaS) services. While you can think of IaaS as direct access to compute infrastructure, PaaS provides ready-made development and deployment environments that are managed for you.

As an example, say you run SQL Server on a VM running on Azure. This configuration requires you to manage the underlying operating system, set up a SQL Server license, manage software and security updates, and so on. You also pay for the VM whether or not the database is processing queries. One way to potentially save costs is to move your database from SQL Server on a VM to Azure SQL Database. Azure SQL Database is based on SQL Server.

Not only are PaaS services such as Azure SQL Database often less expensive to run, but because they're managed for you, you don't need to worry about software updates, security patches, or optimizing physical storage for read and write operations.

Save on licensing costs

Licensing is another area that can dramatically impact your cloud spending. Let's look at some ways you can reduce your licensing costs.

Choose cost-effective operating systems

Many Azure services provide a choice of running on Windows or Linux. In some cases, the cost depends on which you choose. When you have a choice, and your application doesn't depend on the underlying operating system, it's useful to compare pricing to see whether you can save money.

Use Azure Hybrid Benefit to repurpose software licenses on Azure

If you've purchased licenses for Windows Server or SQL Server, and your licenses are covered by Software Assurance , you might be able to repurpose those licenses on VMs on Azure.
Some of the details vary between Windows Server or SQL Server. We'll provide resources at the end of this module where you can learn more.

From <https://docs.microsoft.com/en-us/learn/modules/plan-manage-azure-costs/6-manage-minimize-total-cost>

Choose the right Azure services by examining SLAs and service lifecycle

Thursday, January 28, 2021 10:59 AM

Learn about service-level agreements (SLAs) in Azure, and how they can affect your application design decisions. See how to access preview services and learn how they affect your planning.

Overview

- Introduction 1 min
- What are service-level agreements (SLAs)? 6 min
- Define your application SLA 3 min
- Design your application to meet your SLA 7 min
- Access preview services and preview features 4 min
- Knowledge check 4 min
- Summary 2 min

From <https://docs.microsoft.com/en-us/learn/paths/az-900-describe-azure-cost-management-service-level-agreements/>

Introduction

- 1 minute

In this module, you'll learn about service-level agreements (SLAs) in Azure and how they can affect your application design decisions. You'll also learn about the lifecycle of new Azure services, from preview to general availability.

Meet Tailwind Traders

Tailwind Traders is a fictitious home improvement retailer. It operates retail hardware stores across the globe and online.

Tailwind Traders specializes in competitive pricing, fast shipping, and a large range of items. It's looking at cloud technologies to improve business operations and support growth into new markets. By moving to the cloud, the company plans to enhance its shopping experience to further differentiate itself from competitors.

How will moving to the cloud affect availability

agreements?

Moving to the cloud removes the burden of supporting IT infrastructure. When network connectivity is lost or a hard drive fails, you rely on the cloud provider to restore service. Tailwind Traders' IT department hosts applications and services in its datacenter for the rest of the company. The IT department has agreements with other teams in place that state how available those services will be, which includes when and how planned maintenance can happen. As Tailwind Traders moves its workloads to Azure, it no longer has full control over the hardware and networks. How will its agreements around availability be affected?

Learning objectives

After completing this module, you'll be able to:

- Describe what an SLA is and why SLAs are important.
- Identify factors, such as the service tier you choose, that can affect an SLA.
- Combine SLAs to compute a composite SLA.
- Describe the service lifecycle in Azure, including how to access new capabilities that are coming to Azure.

Prerequisites

- You should be familiar with basic computing concepts and terminology.

From <https://docs.microsoft.com/en-us/learn/modules/choose-azure-services-sla-lifecycle/1-introduction>

What are service-level agreements (SLAs)?

- 6 minutes

A *service-level agreement* (SLA) is a formal agreement between a service company and the customer. For Azure, this agreement defines the performance standards that Microsoft commits to for you, the customer.

In this part, you'll learn more about Azure SLAs, including why SLAs are important, where you can find the SLA for a specific Azure service, and what you'll find in a typical SLA.

Why are SLAs important?

Understanding the SLA for each Azure service you use helps you understand what guarantees you can expect.

When you build applications on Azure, the availability of the services that you use affect your application's performance. Understanding the SLAs involved can help you establish the SLA you set with your customers.

Later in this module, you'll learn about some strategies you can use when an Azure SLA doesn't meet your needs.

Where can I access SLAs for Azure services?

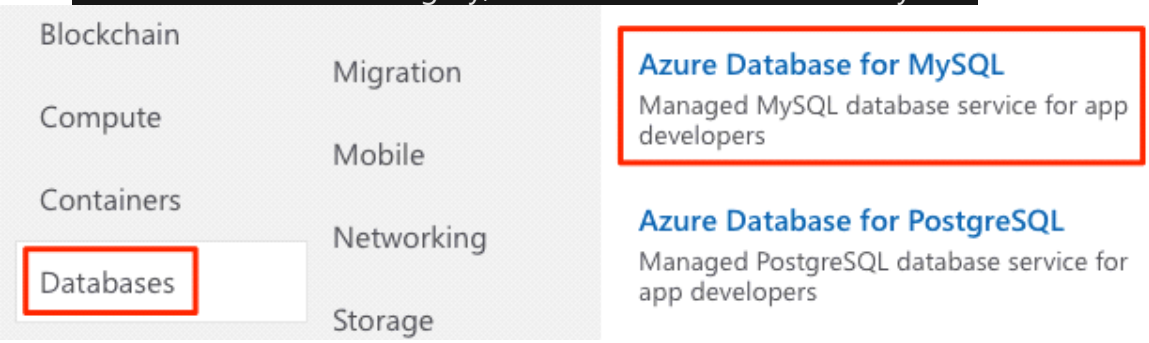
You can access SLAs from Service Level Agreements .

Note

You don't need an Azure subscription to review service SLAs.

Each Azure service defines its own SLA. Azure services are organized by category. Open the SLA for Azure Database for MySQL, a managed database that makes it easy for developers to work with MySQL databases. You'll refer back to this SLA in a moment. To do so:

1. Go to Service Level Agreements .
2. From the Databases category, select Azure Database for MySQL.



What's in a typical SLA?

A typical SLA breaks down into these sections:

- Introduction
  This section explains what to expect in the SLA, including its scope and how subscription renewals can affect the terms.
- General terms
  This section contains terms that are used throughout the SLA so that both parties (you and Microsoft) have a consistent vocabulary. For example, this section might define what's meant by downtime, incidents, and error codes.
  This section also defines the general terms of the agreement, including how to submit a claim, receive credit for any performance or availability issues, and limitations of the agreement.
- SLA details
  This section defines the specific guarantees for the service. Performance commitments are commonly measured as a percentage. That percentage typically ranges from 99.9 percent ("three nines") to 99.99 percent ("four nines").
  The primary performance commitment typically focuses on *uptime*, or the percentage of time that a product or service is successfully operational. Some SLAs focus on other factors as well, including *latency*, or how fast the service must respond to a request.

This section also defines any additional terms that are specific to this service.
Take a moment to review the SLA for Azure Database for MySQL.
You see that this SLA focuses mainly on uptime. Azure Database for MySQL guarantees 99.99 percent, or "four nines", uptime. This means that the service is guaranteed to be running and available to process requests 99.99 percent of the time.

How do percentages relate to total downtime?

Downtime refers to the time duration that the service is unavailable.
The difference between 99.9 percent and 99.99 percent might seem minor, but it's important to understand what these numbers mean in terms of total downtime.
Here's a table to give you a sense of how total downtime decreases as the SLA percentage increases from 99 percent to 99.999 percent:

SLA percentage	Downtime per week	Downtime per month	Downtime per year
99	1.68 hours	7.2 hours	3.65 days
99.9	10.1 minutes	43.2 minutes	8.76 hours
99.95	5 minutes	21.6 minutes	4.38 hours
99.99	1.01 minutes	4.32 minutes	52.56 minutes
99.999	6 seconds	25.9 seconds	5.26 minutes

HOW DO PERCENTAGES RELATE TO TOTAL DOWNTIME?

These amounts are cumulative, which means that the duration of multiple different service outages would be combined, or added together.

What are service credits?

A *service credit* is the percentage of the fees you paid that are credited back to you according to the claim approval process.
An SLA describes how Microsoft responds when an Azure service fails to perform to its specification. For example, you might receive a discount on your Azure bill as compensation when a service fails to perform according to its SLA.
Credits typically increase as uptime decreases. Here's how credits are applied for Azure Database for MySQL according to uptime:

Monthly uptime percentage	Service credit percentage
< 99.99	10
< 99	25
< 95	100

WHAT ARE SERVICE CREDITS?

What's the SLA for free services?

Free products typically don't have an SLA.

For example, many Azure services provide a *free* or *shared* tier that provides more limited functionality. Services like Azure Advisor are always free. The SLA for Azure Advisor states that because it's free, it doesn't have a financially backed SLA.

How do I know when there's an outage?

Azure status provides a global view of the health of Azure services and regions. If you suspect there's an outage, this is often a good place to start your investigation.
Azure status provides an RSS feed of changes to the health of Azure services that you can subscribe to. You can connect this feed to communication software such as Microsoft Teams or Slack.
From the Azure status page, you can also access Azure Service Health. This provides a personalized view of the health of the Azure services and regions that you're using, directly from the Azure portal.

How can I request a service credit from Microsoft?

Typically, you need to file a claim with Microsoft to receive a service credit. If you purchase Azure services from a Cloud Solution Provider (CSP) partner, your CSP typically manages the claims process.
Each SLA specifies the timeline by which you must submit your claim and when Microsoft processes your claim. For many services, you must submit your claim by the end of the calendar month following the month in which the incident occurred.
Next, let's look at some other factors that Tailwind Traders needs to consider that might affect SLA performance targets.

From <https://docs.microsoft.com/en-us/learn/modules/choose-azure-services-sla-lifecycle/2-what-are-service-level-agreements>

Define your application SLA

- 3 minutes

An *application SLA* defines the SLA requirements for a specific application. This term typically refers to an application that *you* build on Azure.
Tailwind Traders runs an application that it built on Azure called "Special Orders." The application tracks special orders that customers have placed in the company's retail stores. A special order includes an item and any customizations the customer needs. For example, a folding door might include customizations such as dimension and hinge placement. Because customizations typically require special handling, the customized item needs to be ordered from the supplier when a customer needs it.
There are many design decisions you can make to improve the availability and resiliency of the applications and services you build on Azure. These decisions extend beyond just the SLA for a specific service. In this part, you'll explore a few of these considerations.

A good place to start is to have a discussion with your team about how important the availability of each application is to your business. The following sections cover a few factors that Tailwind Traders might consider.

Business impact

If the Special Orders application goes down, what would the business impact be? In this case, customers can't place new orders through the store and staff can't check the status of existing orders. Customers will either need to try again later or possibly go to a competitor.

Effect on other business operations

The Special Orders application doesn't affect other operations. So the majority of the Tailwind Traders business will continue to function normally if the Special Orders application went down.

Usage patterns

Usage patterns define when and how users access your application.
One question to consider is whether the availability requirement differs between critical and non-critical time periods. For example, a tax-filing application can't fail during a filing deadline.
For Tailwind Traders, retail stores aren't open 24 hours a day, so if the application were down in the middle of the night, the impact would be minimal. However, because Tailwind Traders has retail locations all over the world, it will need to ensure that each location has access to the service during its retail hours.

What does the team decide?

Let's say that Tailwind Traders decides that an SLA of 99.9 percent is acceptable for the Special Orders application. This gives the company an estimated downtime of 10.1 minutes per week. But how will it ensure that its technology choices support its application SLA?
In the next part, you'll see how the team maps its application requirements to specific Azure services. You'll learn about some of the techniques you can use to help ensure that your technology choices meet your application SLA.

From <https://docs.microsoft.com/en-us/learn/modules/choose-azure-services-sla-lifecycle/3-define-application-sla>

Design your application to meet your SLA

- 7 minutes

Tailwind Traders decides that an SLA of 99.9 percent is acceptable for the Special Orders application. Recall that this gives the company an estimated downtime of 10.1 minutes per week.

Now you need to design an efficient and reliable solution for this application on Azure, keeping that application SLA in mind. You'll select the Azure products and services you need, and provision your cloud resources according to those requirements.

In reality, failures will happen. Hardware can fail. The network can have intermittent timeout periods. While it's rare for an entire service or region to experience a disruption, you still need to plan for such events.

Let's follow the process Tailwind Traders uses to ensure that its technology choices meet its application SLA.

Identify your workloads

A *workload* is a distinct capability or task that's logically separated from other tasks, in terms of business logic and data storage requirements. Each workload defines a set of requirements for availability, scalability, data consistency, and disaster recovery.

On Azure, the Special Orders application will require:

- Two virtual machines.
- One instance of Azure SQL Database.
- One instance of Azure Load Balancer.

Here's a diagram that shows the basic architecture:

Combine SLAs to compute the composite SLA

After you've identified the SLA for the individual workloads in the Special Orders application, you might notice that those SLAs are not all the same. How does this affect our overall application SLA requirement of 99.9 percent? To work that out, you'll need to do some math.

The process of combining SLAs helps you compute the *composite SLA* for a set of services. Computing the composite SLA requires that you multiply the SLA of each individual service.

From Service Level Agreements , you discover the SLA for each Azure service that you need. They are:

Service	SLA
Azure Virtual Machines	99.9 percent
Azure SQL Database	99.99 percent
Azure Load Balancer	99.99 percent

COMBINE SLAS TO COMPUTE THE COMPOSITE SLA

Therefore, for the Special Orders application, the composite SLA would be: 99.9%×99.9%×99.99%×99.99%99.9%×99.9%×99.99%×99.99%=0.999×0.999×0.9999×0.9999=0.999×0.999×0.9999×0.9999=0.9978=0.9978=99.78%=

99.78%
Recall that you need two virtual machines. Therefore, you include the Virtual Machines SLA of 99.9 percent two times in the formula.
Note that even though all of the individual services have SLAs equal to or better than the application SLA, combining them results in an overall number that's *lower* than the 99.9 percent you need. Why? Because using multiple services adds an extra level of complexity and slightly increases the risk of failure.
You see here that the composite SLA of 99.78 percent doesn't meet the required SLA of 99.9 percent. You might go back to team and ask whether this is acceptable. Or you might implement some other strategies into your design to improve this SLA.

What happens when the composite SLA doesn't meet your needs?

For the Special Orders application, the composite SLA of doesn't meet the required SLA of 99.9 percent. Let's look at a few strategies that Tailwind Traders might consider.

Choose customization options that fit your required SLA

Each of the workloads defined previously has its own SLA, and the customization choices you make when you provision each workload affects that SLA. For example:

- Disks
  With Virtual Machines, you can choose from a Standard HDD Managed Disk, a Standard SSD Managed Disk, or a Premium SSD or Ultra Disk. The SLA for a single VM would be either 95 percent, 99.5 percent or 99.9 percent, depending on the disk choice.
- Tiers
  Some Azure services are offered as both a free tier product and as a standard paid service. For example, Azure Automation provides 500 minutes of job runtime in an Azure free account, but is not backed by an SLA. The standard tier SLA for Azure Automation is 99.9 percent.

Make sure that your purchasing decisions take into account the impact on the SLA for the Azure services that you choose. Doing so ensures that the SLA supports your required application SLA.
Here, Tailwind Traders might choose the Ultra Disk option for its virtual machines to help guarantee greater uptime.

Build availability requirements into your design

There are application design considerations you can use that relate to the underlying cloud infrastructure.
For example, to improve the availability of the application, avoid having any single

points of failure. So instead of adding more virtual machines, you can deploy one or more extra instances of the same virtual machine across the different availability zones in the same Azure region.
An *availability zone* is a unique physical location within an Azure region. Each zone is made up of one or more datacenters equipped with independent power, cooling, and networking. These zones use different schedules for maintenance, so if one zone is affected, your virtual machine instance in the other zone is unaffected.
Deploying two or more instances of an Azure virtual machine across two or more availability zones raises the virtual machine SLA to 99.99 percent. Recalculating your composite SLA above with this Virtual Machines SLA gives you an application SLA of: 99.99%×99.99%×99.99%×99.99%99.99%×99.99%×99.99%×99.99%=99.96%=99.96%
This revised SLA of 99.96 percent exceeds your target of 99.9 percent.
To learn more about the SLA for Virtual Machines, visit SLA for Virtual Machines .

Include redundancy to increase availability

To ensure high availability, you might plan for your application to have duplicate components across several regions, known as *redundancy*. Conversely, to minimize costs during non-critical periods, you might run your application only in a single region. Tailwind Traders might consider this if there's a trend that the special order rates are much higher during certain months or seasons.
To achieve maximum availability in your application, add redundancy to every single part of the application. This redundancy includes the application itself, as well as the underlying services and infrastructure. Be aware, however, that doing so can be difficult and expensive, and often results in solutions that are more complex than they need to be.
Consider how critical high availability is to your requirements before you add redundancy. There may be simpler ways to meet your application SLA.

Very high performance is difficult to achieve

Performance targets above 99.99 percent are very difficult to achieve. An SLA of 99.99 percent means 1 minute of downtime per week. It's difficult for humans to respond to failures quickly enough to meet SLA performance targets above 99.99 percent. Instead, your application must be able to self-diagnose and self-heal during an outage.

From <https://docs.microsoft.com/en-us/learn/modules/choose-azure-services-sla-lifecycle/4-design-application-meet-sla>

Access preview services and preview features

- 4 minutes

Now that Tailwind Traders has its applications up and running, it wants to start looking

into new capabilities. One option is to look at preview services. In this part, you'll learn how Azure services go from the preview phase to being generally available.

For Tailwind Traders, migration from the datacenter to Azure is more about operational efficiency. The research and development team is looking into new, cloud-based features that will keep them ahead of the competition.

Tailwind Traders is experimenting with a custom drone delivery system for customers in rural areas. The company needs the ability to use real-time storm tracking in the drone guidance system, but the feature isn't ready yet. There's a new AI Storm Analyzer service that has just entered the public preview phase. So Tailwind Traders has decided to incorporate it into the early stages of application testing.

Note

AI Storm Analyzer is a fictitious Azure service, introduced here for illustration purposes only.

Before the team moves forward, it wants a better understanding of how preview services affect its SLA. Let's begin by defining the Azure service lifecycle.

What is the service lifecycle?

The *service lifecycle* defines how every Azure service is released for public use.

Every Azure service starts in the development phase. In this phase, the Azure team collects and defines its requirements, and begins to build the service.

Next, the service is released to the public preview phase. During this phase, the public can access and experiment with it so that it can provide feedback. Your feedback helps Microsoft improve services. More importantly, providing feedback gives you the opportunity to request new or different capabilities so that services better meet your needs.

After a new Azure service is validated and tested, it's released to all customers as a production-ready service. This is known as *general availability* (GA).

What terms and conditions can I expect?

Each Azure preview defines its own terms and conditions. All preview-specific terms and conditions supplement your existing Azure service agreement.

Some previews aren't covered by customer support. Therefore, previews are not recommended for business-critical workloads.

How can I access preview services?

You can access preview services from the Azure portal.

Here's how to see what preview services are available. You can follow along if you have an Azure subscription.

1. Go to the Azure portal and sign in.
2. Select Create a resource.

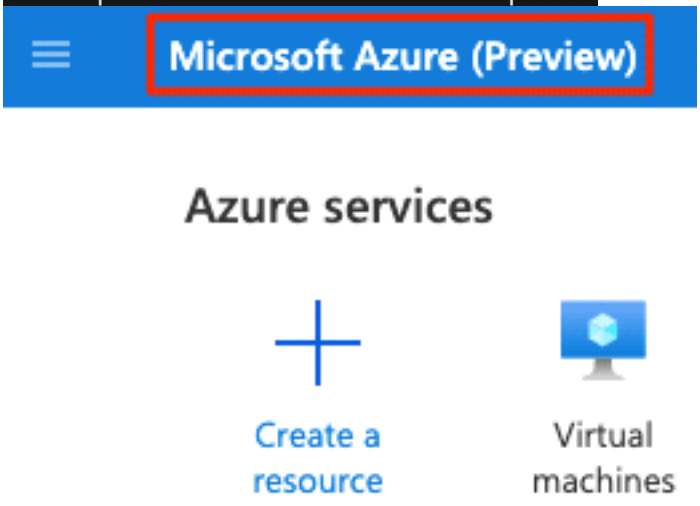
3. Enter *preview* in the search box, and select Enter.
4. Select a service to learn more about it. You can also launch the service if you'd like to try it out.

How can I access new features for an existing service?

Some preview features relate to a specific area of an existing Azure service. For example, a compute or database service that you use daily might provide enhanced functionality. These preview features are accessible when you deploy, configure, and manage the service.
Although you can use an Azure preview feature in production, make sure you're aware of any limitations around its use before you deploy it to production.

How can I access preview features for the Azure portal?

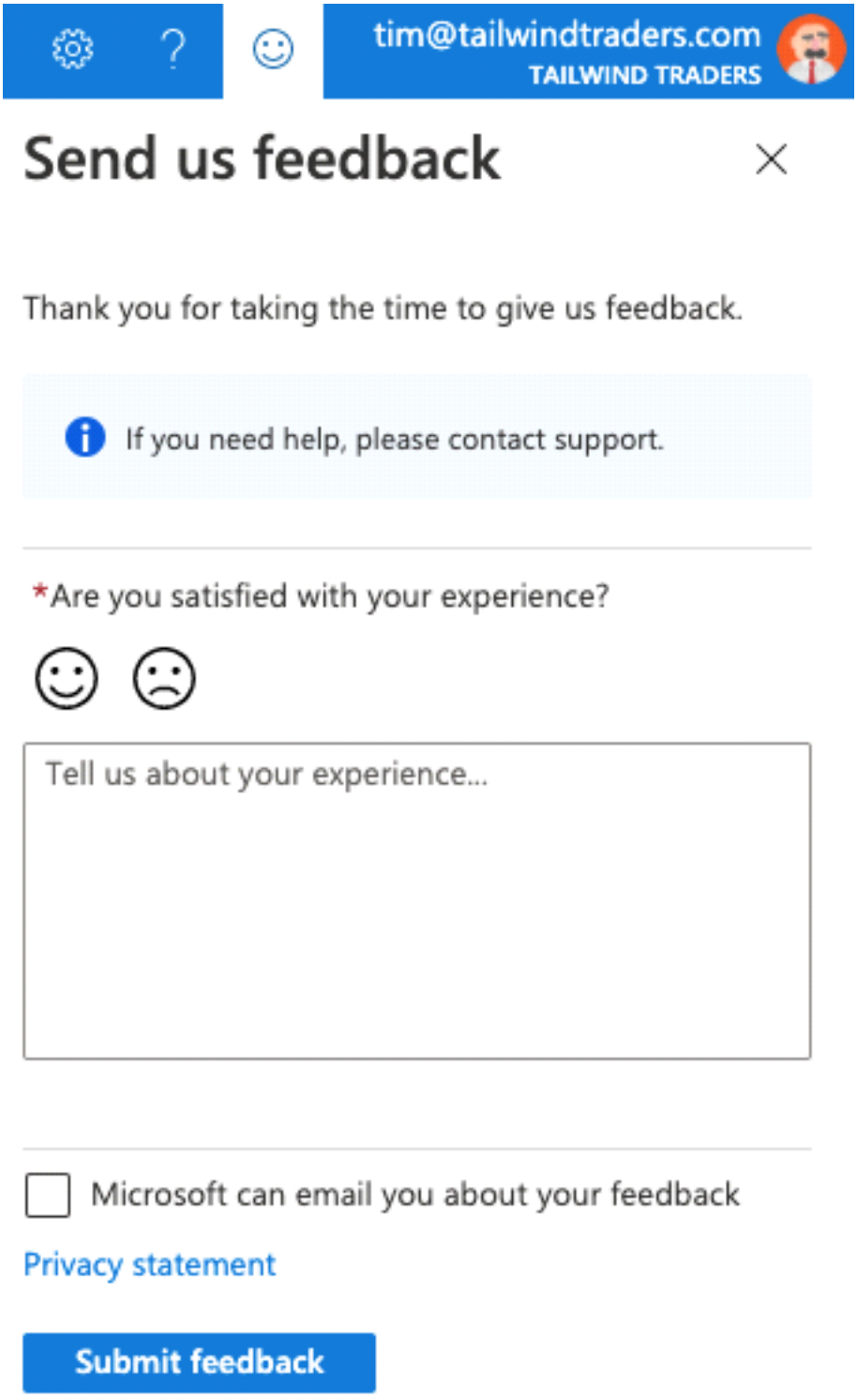
You can access preview features that are specific to the Azure portal from Microsoft Azure (Preview) .
Typical portal preview features provide performance, navigation, and accessibility improvements to the Azure portal interface.
You see Microsoft Azure (Preview) near the menu bar to remind you that you're working with a preview version of the Azure portal.



How can I provide feedback on the Azure portal?

You can provide feedback:

- From the Feedback tab in the Azure portal.



- From the Azure portal feedback forum .

How can I stay updated on the latest announcements?

The Azure updates page provides information about the latest updates to Azure products, services, and features, as well as product roadmaps and announcements. From the Azure updates page, you can:

- View details about all Azure updates.
- See which updates are in general availability, preview, or development.

- Browse updates by product category or update type.
- Search for updates by keyword.
- Subscribe to an RSS feed to receive notifications.
- Access the Microsoft Connect page to read Azure product news and announcements.

From <https://docs.microsoft.com/en-us/learn/modules/choose-azure-services-sla-lifecycle/5-access-preview-services>