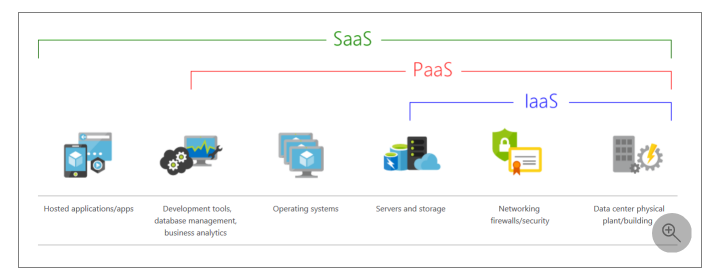
**Azure cloud training by Microsoft**

**What are cloud service models?**

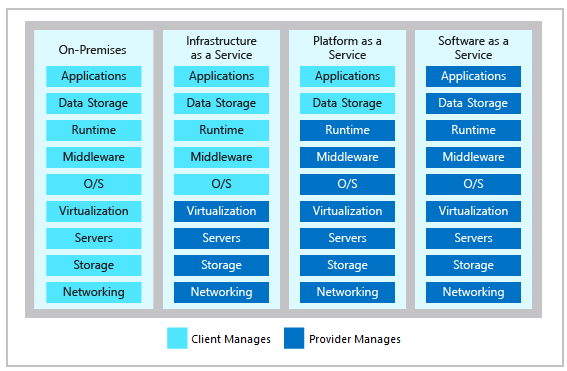
Cloud computing falls into one of the following computing models. If you've been around cloud computing for a while, you've probably seen the terms infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS) for the different cloud service models. These models define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

| **What are cloud service models?** | |
| --- | --- |
| **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. |

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 server-less 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.

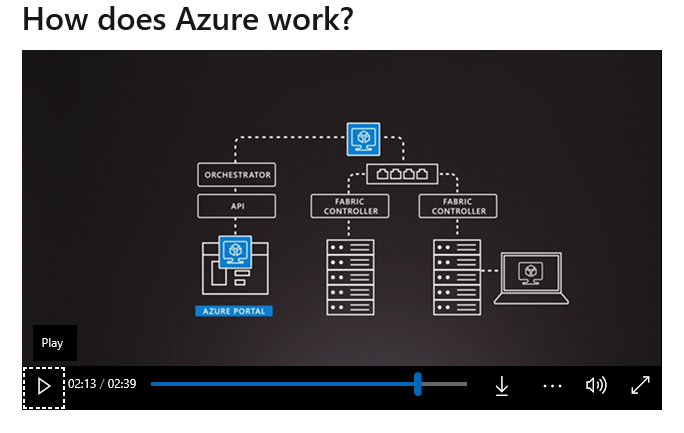
In understanding the definition of serverless computing, it's important to note that servers are still running the code. The **serverless name comes from the fact that the tasks associated with infrastructure provisioning and management are invisible to the developer**. This approach enables developers 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.

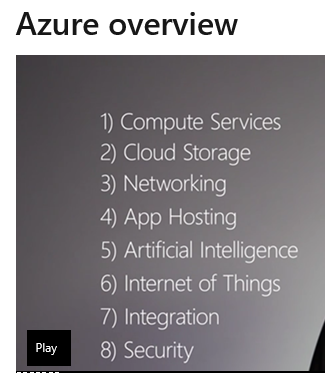
**What are public, private, and hybrid clouds?**

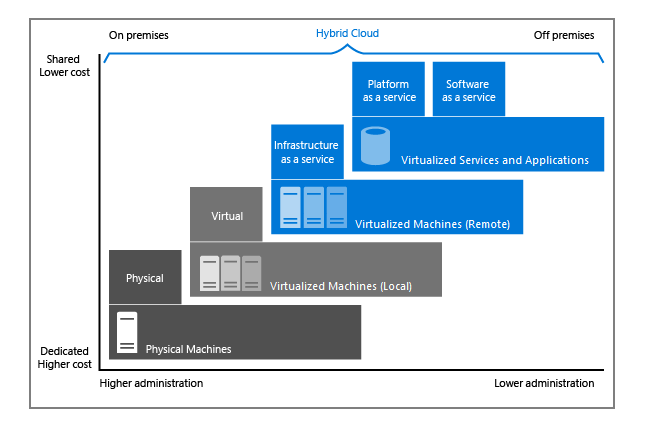
There are three deployment models for cloud computing: *public cloud*, *private cloud*, and *hybrid cloud*. Each deployment model has different aspects that you should consider as you migrate to the cloud.

| **What are public, private, and hybrid clouds?** | |
| --- | --- |
| **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 cloud** | Computing resources are used exclusively by users from one business or organization. A 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. |

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.







**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.

| **Table 1** | |
| --- | --- |
| **Service name** | **Service function** |
| Azure Virtual Machines | Windows or Linux virtual machines (VMs) hosted in Azure |
| Azure Virtual Machine Scale Sets | Scaling for Windows or Linux VMs hosted in Azure |
| 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 |

**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 |

**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 |

### 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.
* Auto-scaling 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.

| **Table 4** | |
| --- | --- |
| **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 (**RDBM**) |
| **Azure Database for MySQL** | Fully managed and scalable MySQL relational database with high availability and security (**RDBM**) |
| **Azure Database for PostgreSQL** | Fully managed and scalable PostgreSQL relational database with high availability and security (**RDBM**) |
| 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 (RDBM) |

**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.

| **Table 5** | |
| --- | --- |
| **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. |

**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.

| **Table 6** | |
| --- | --- |
| **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 |

**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.

| **Table 7** | |
| --- | --- |
| **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. |

**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.

| **Table 8** | |
| --- | --- |
| **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 Machine Learning Studio | Collaborative visual workspace where you can build, test, and deploy machine learning solutions by using prebuilt machine learning algorithms and data-handling modules. |

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

| **Table 9** | |
| --- | --- |
| **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. |

**DevOps**

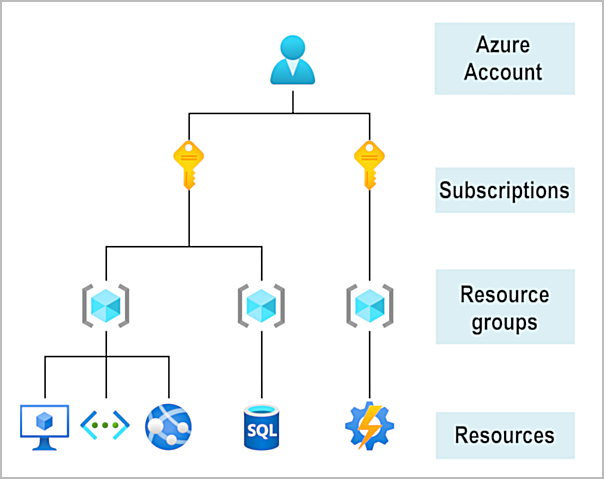
DevOps brings together people, processes, and technology by automating software delivery to provide continuous value to your users. With Azure DevOps, you can create *build* and *release* pipelines that provide continuous integration, delivery, and deployment for your applications. You can integrate 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.

| **Table 10** | |
| --- | --- |
| **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. |

**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.

[](https://docs.microsoft.com/en-us/learn/azure-fundamentals/intro-to-azure-fundamentals/media/scope-levels-expanded.png#lightbox)

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.

**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?**

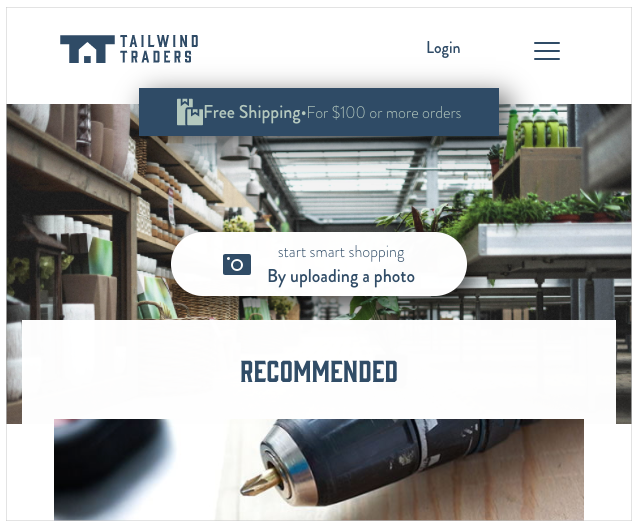
Many of the Learn exercises use a technology called the sandbox, which creates a temporary subscription that's added to your Azure account. This temporary subscription allows you to create Azure resources for the duration of a Learn module. Learn automatically cleans up the temporary resources for you 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.

**Case study introduction**

* 2 minutes

Throughout the Azure Fundamentals learning paths, we'll work with [Tailwind Traders](https://www.tailwindtraders.com/?) , a fictitious home improvement retailer. It operates retail hardware stores across the globe and online.

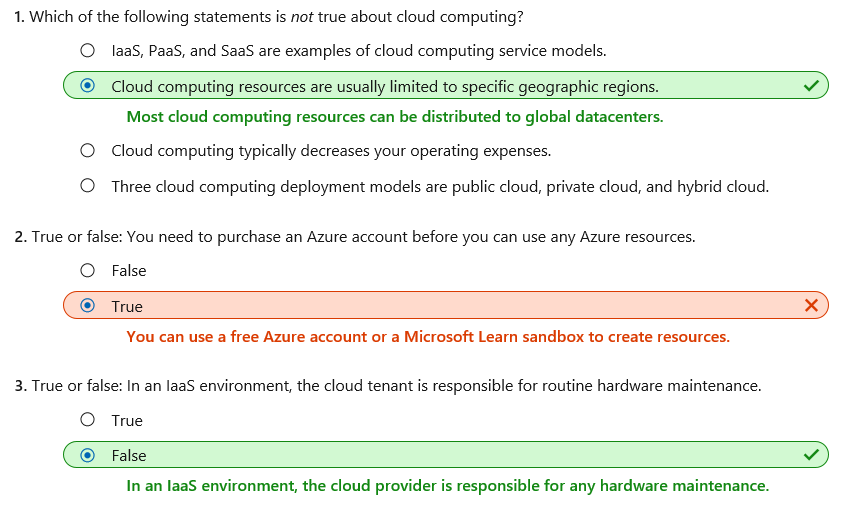


Tailwind Traders currently manages an on-premises datacenter that hosts the company's retail website. The datacenter also stores all of the data and streaming video for its applications. The IT department is currently responsible for all of the management tasks for its computing hardware and software. 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.



**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.

**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.

**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.

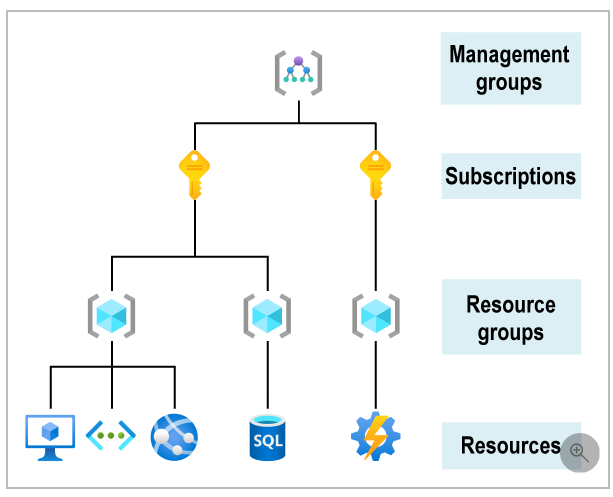
Cloud services, on the other hand, are categorized as an OpEx, because of their consumption model. There's no asset for Tailwind Traders to amortize, and its cloud service provider (Azure) manages the costs that are associated with the purchase and lifespan of the physical equipment. As a result, OpEx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

**Azure Database services**

* Azure Cosmos DB
* Azure SQL Database
* Azure SQL Managed Instance
* Azure Database for MySQL
* Azure Database for PostgreSQL
* Azure Synapse Analytics
* Azure HDInsight
* Azure Data bricks
* Azure Data Lake Analytics

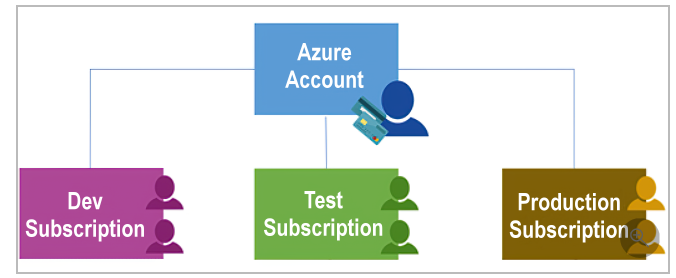
**Overview of Azure subscriptions, management groups, resources, and regions**



* **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.

## 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.

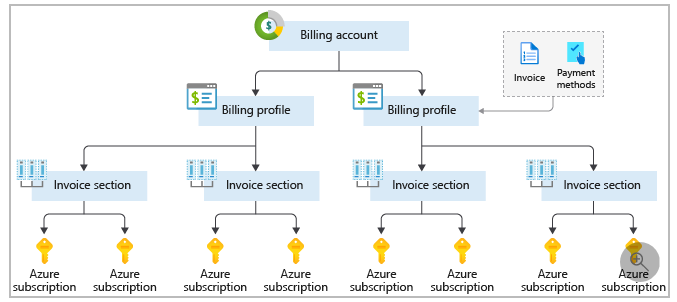


Note: An account can have one subscription or multiple subscriptions that have different billing models and to which you apply different access-management policies. You can use Azure subscriptions to define boundaries around Azure products, services, and resources.

There are two types of subscription boundaries that you can use:

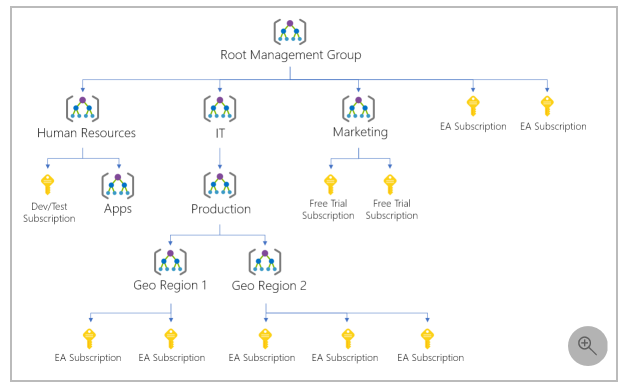
1.**Billing boundary**

2.**Access control boundary**



**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.



**Important facts about management groups**

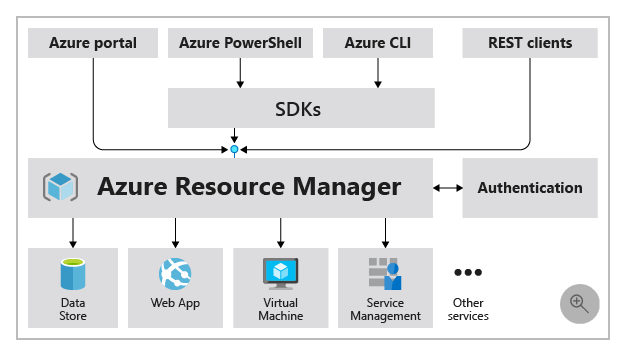
* 10,000 management groups can be supported in a single directory.
* A management group tree can support up to six levels of depth. This limit doesn't include the root level or the subscription level.
* Each management group and subscription can support only one parent.
* Each management group can have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

## 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. 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.

The benefits of using Resource Manager

* 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.



**Azure regions and availability zones**

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.

## 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.

**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.

**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:

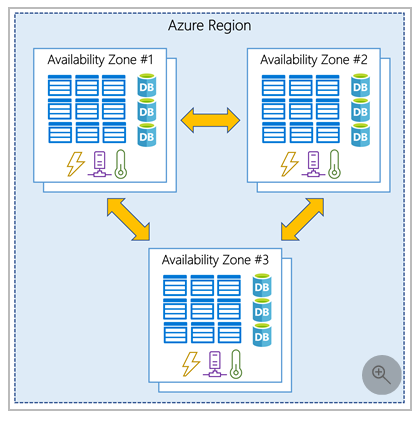
* **US DoD Central, US Gov Virginia, US Gov Iowa and more:** These regions are physical and logical network-isolated instances of Azure for U.S. government agencies and partners. These datacenters are operated by screened U.S. personnel and include additional compliance certifications.
* **China East,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

## 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.



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).

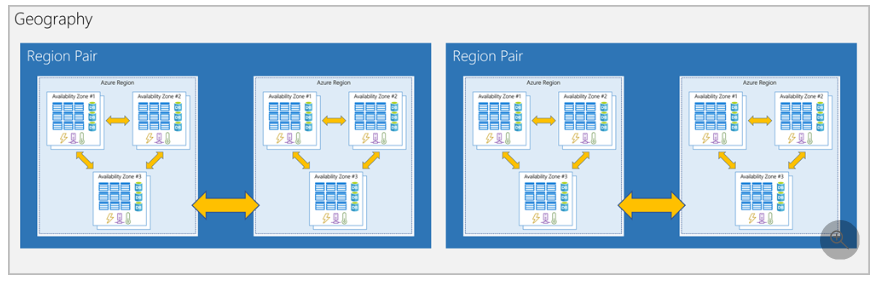
## Azure region pairs

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.



**Exercise - Create a website hosted in Azure**

**Azure terminology and concepts**

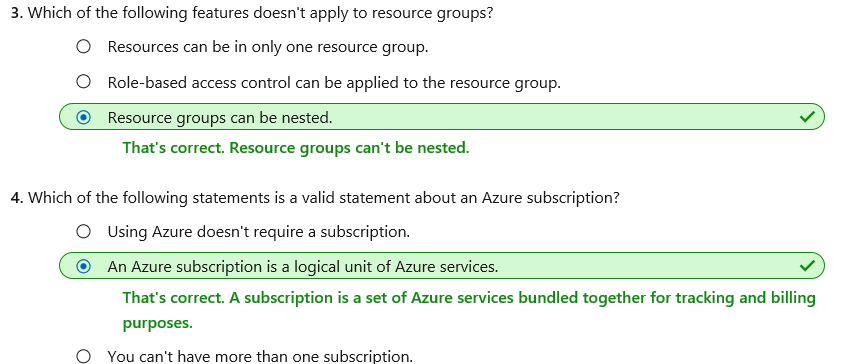
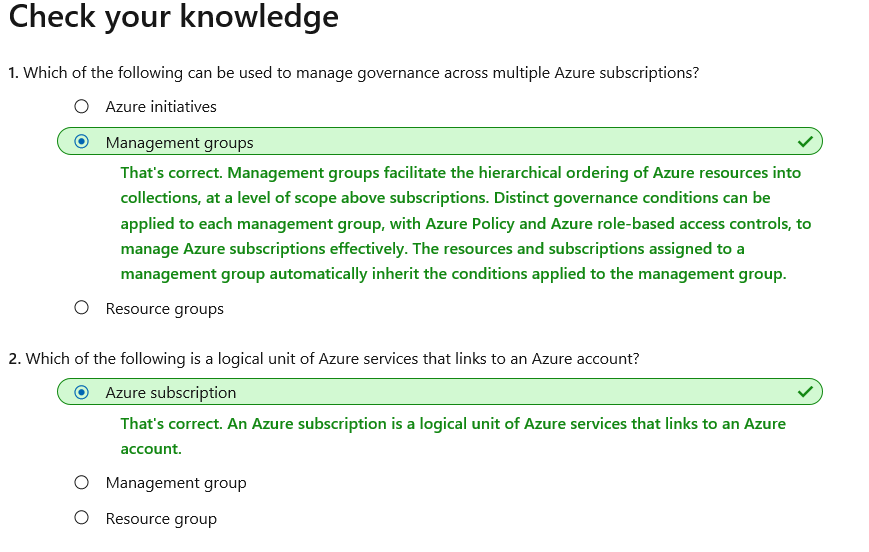
Before you get started, let's review and discuss some basic terms and concepts that you'll need to know when you create your website.

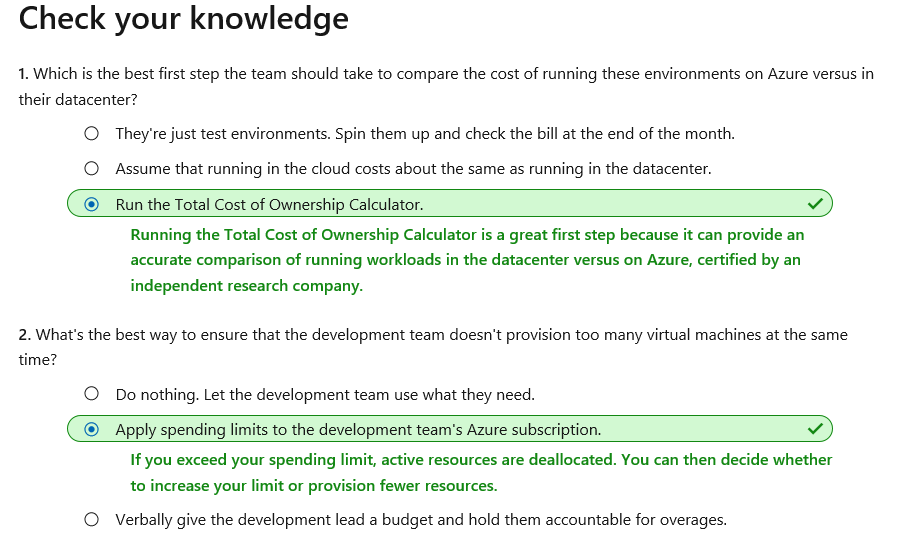
**What is App Service?**

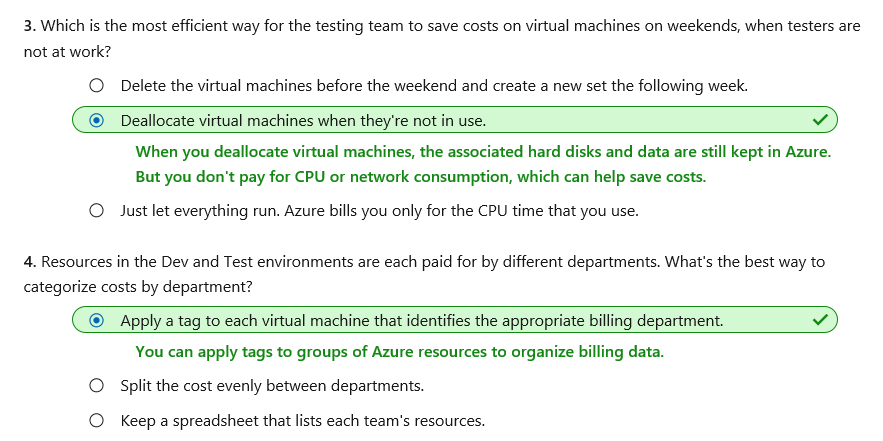
App Service is an HTTP-based service that enables you to build and host many types of web-based solutions without managing infrastructure. For example, you can host web apps, mobile back ends, and RESTful APIs in several supported programming languages. Applications developed in .NET, .NET Core, Java,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

**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.



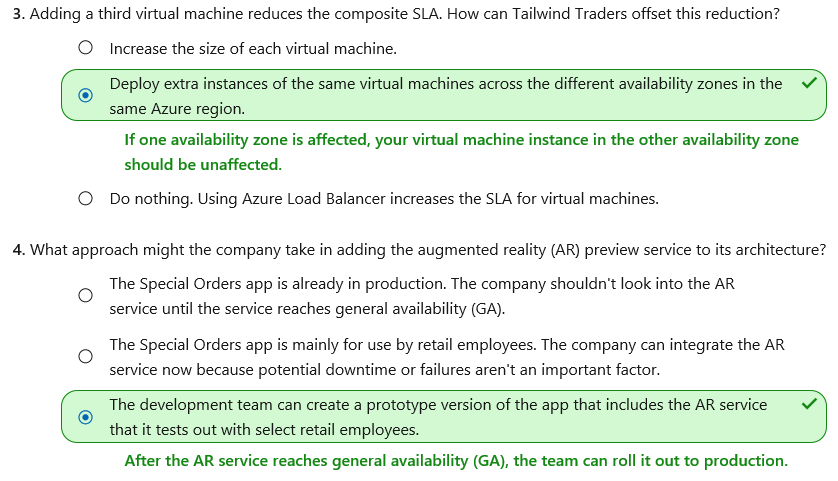
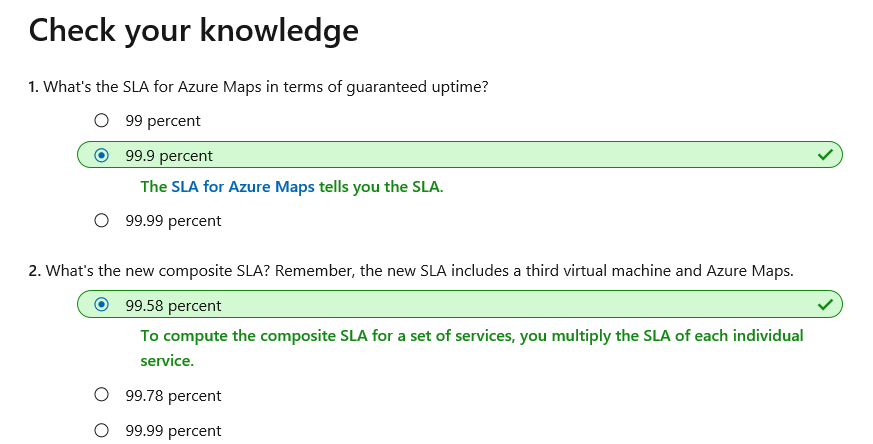




**Note:** The team also created a checklist of cost-saving measures that it can use to help keep down costs. This list includes:

* Perform cost analysis before you deploy.
* Use Azure Advisor to monitor your usage.
* Use spending limits to prevent accidental spending.
* Use Azure Reservations to prepay.
* Choose low-cost locations and regions.
* Research available cost-saving offers.
* Apply tags to identify cost owners.

With these measures in place, the Tailwind Traders team is ready to take the next steps toward cloud migration.



**Azure Cognitive Services**

[Azure Cognitive Services](https://azure.microsoft.com/services/cognitive-services/?) provides prebuilt machine learning models that enable applications to see, hear, speak, understand, and even begin to reason.

**Azure Bot Service**

[Azure Bot Service](https://azure.microsoft.com/services/bot-service/?) and [Bot Framework](https://dev.botframework.com/?) 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.

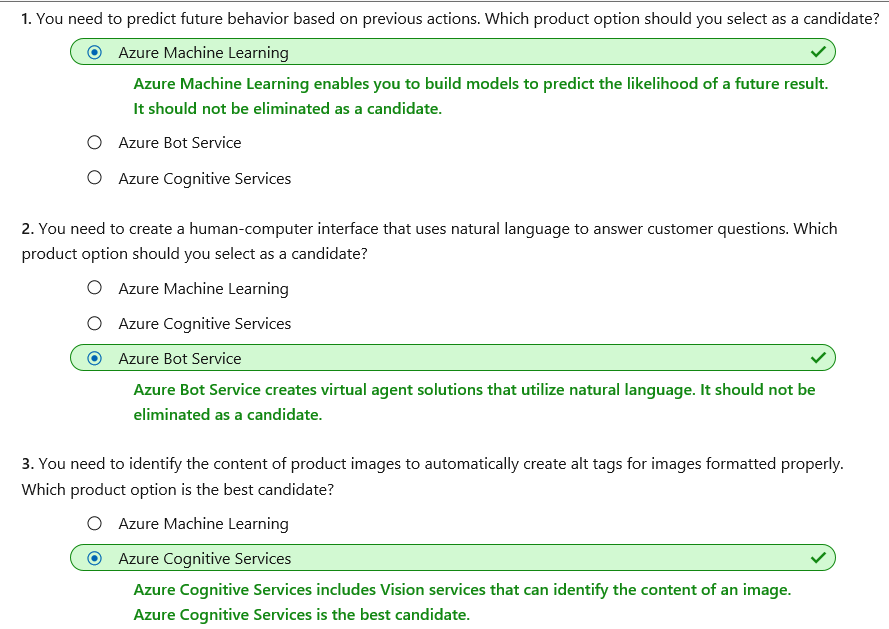
## Are you building a virtual agent that interfaces with humans via natural language?

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.

## 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.



Explore Azure database for MySQL

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.

**Explore Azure Database for PostgreSQL**

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.
* **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.

Explore big data and analytics

## Azure Synapse Analytics

[Azure Synapse Analytics](https://docs.microsoft.com/en-us/azure/sql-data-warehouse/?) (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**

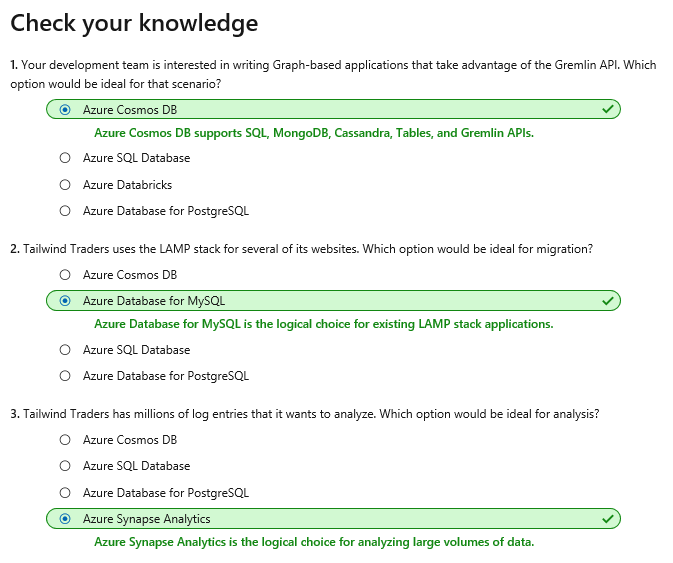
[Azure HDInsight](https://azure.microsoft.com/services/hdinsight/?) is a fully managed, open-source analytics service for enterprises. It's a cloud service that makes it easier, faster, and more cost-effective to process massive amounts of data. You can run popular open-source frameworks and create cluster types such as [Apache Spark](https://docs.microsoft.com/en-us/azure/hdinsight/spark/apache-spark-overview?), [Apache Hadoop](https://docs.microsoft.com/en-us/azure/hdinsight/hadoop/apache-hadoop-introduction?), [Apache Kafka](https://docs.microsoft.com/en-us/azure/hdinsight/kafka/apache-kafka-introduction?), [Apache HBase](https://docs.microsoft.com/en-us/azure/hdinsight/hbase/apache-hbase-overview?), [Apache Storm](https://docs.microsoft.com/en-us/azure/hdinsight/storm/apache-storm-overview?), and [Machine Learning Services](https://docs.microsoft.com/en-us/azure/hdinsight/r-server/r-server-overview?). 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](https://azure.microsoft.com/services/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](https://azure.microsoft.com/services/data-lake-analytics/?)

[Azure Data Lake Analytics](https://azure.microsoft.com/services/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.



**AZURE COMPUTE SERVICES**

**Azure Container Instances or Azure Kubernetes Service**

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.

**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](https://azure.microsoft.com/services/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](https://azure.microsoft.com/services/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.

## Types of app services

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

* Web apps
* API apps
* WebJobs
* Mobile apps

### 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.

# When to use Azure Functions

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.

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.

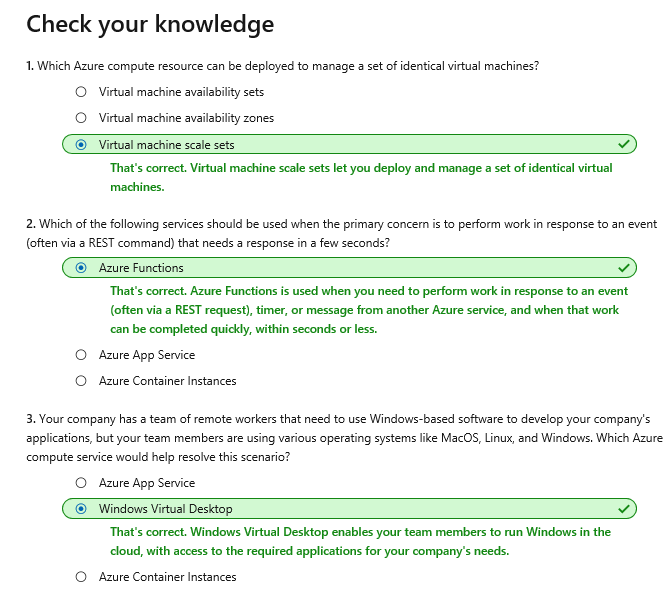
Functions scale automatically based on demand, so they're a solid choice when demand is variable. For example, you might receive messages from an IoT solution that's used to monitor a fleet of delivery vehicles. You'll likely have more data arriving during business hours.

## 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.

## 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.

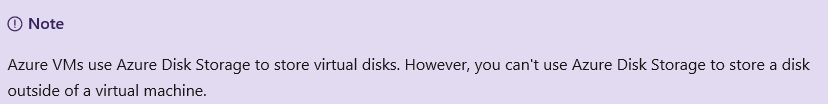


**Azure storage services**

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

**Azure Storage account fundamentals**

[Azure Storage](https://azure.microsoft.com/product-categories/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.



Disk storage fundamentals

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.

Azure Blob storage fundamentals

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.

Blob Storage is ideal for:

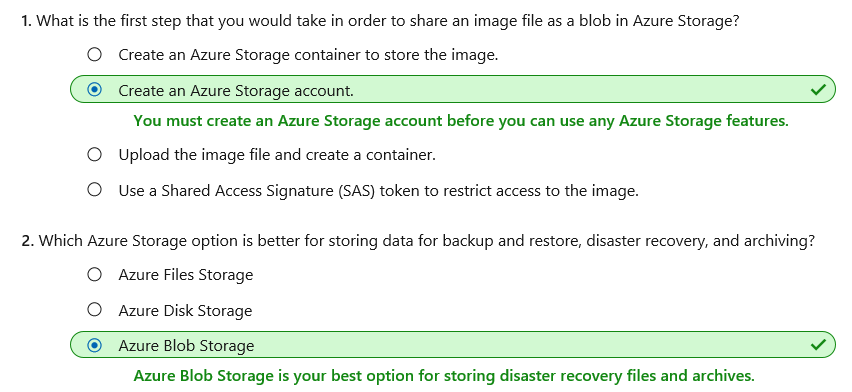
* Serving images or documents directly to a browser.
* Storing files for distributed access.
* Streaming video and audio.
* Storing data for backup and restore, disaster recovery, and archiving.
* Storing data for analysis by an on-premises or Azure-hosted service.
* Storing up to 8 TB of data for virtual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

Azure Files fundamentals

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.

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).



Azure Virtual Network fundamentals

**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.

### 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.

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.

Azure VPN Gateway fundamentals

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.

## 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.

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.

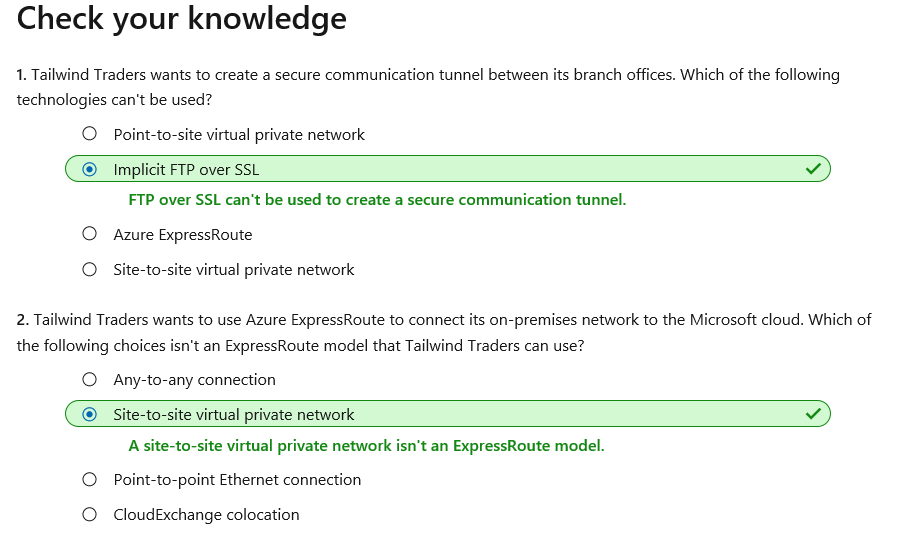
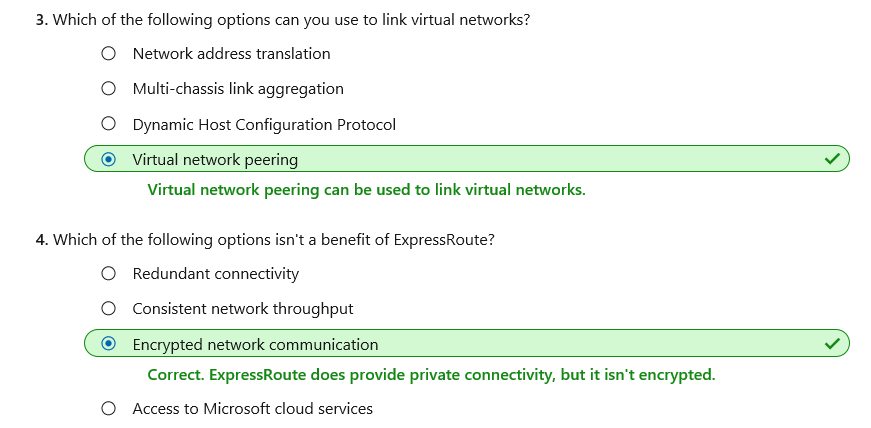
Azure ExpressRoute fundamentals

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.

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.

Understand your product options

## 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.

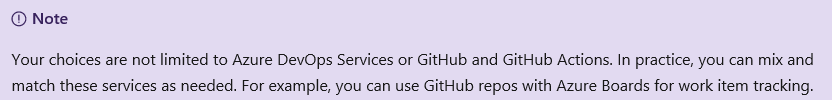
### Azure DevOps Services

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.

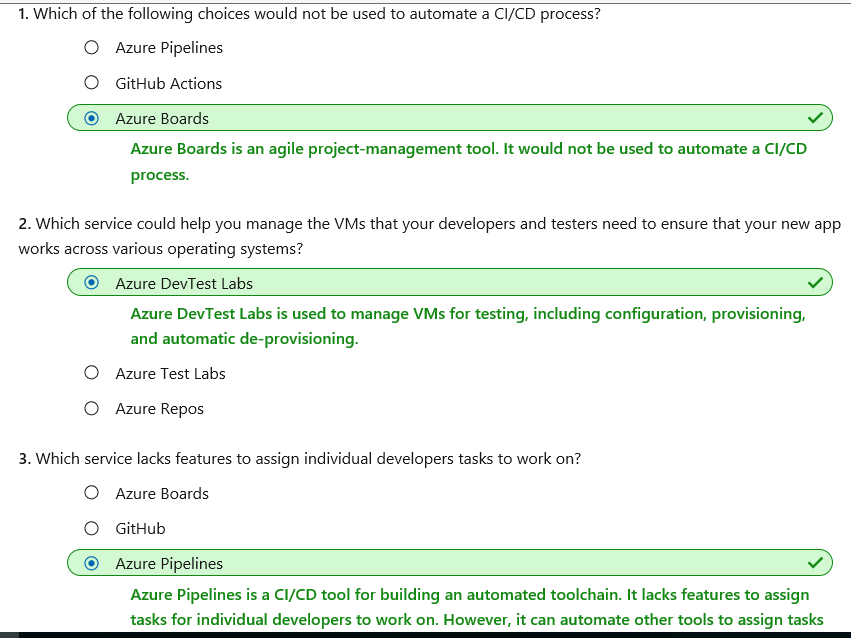
### GitHub and GitHub Actions

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.



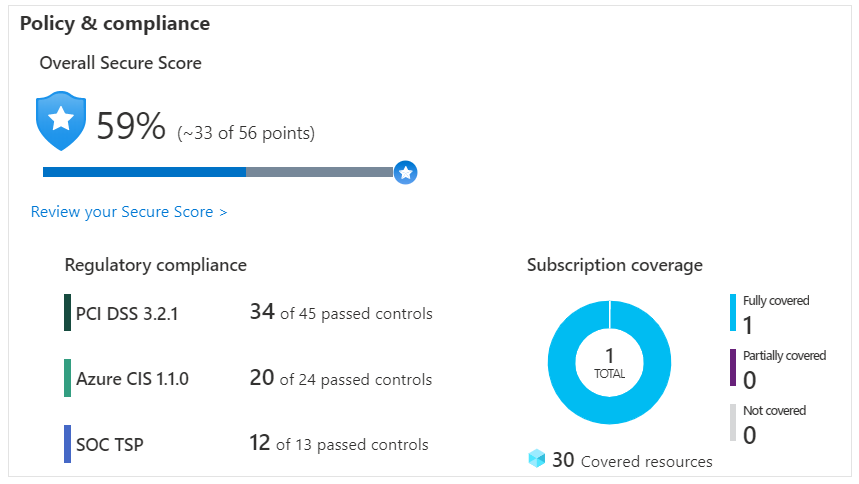
### Azure DevTest Labs

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.



## What's Azure Security Center?

[Azure Security Center](https://azure.microsoft.com/services/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.



## 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.

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.

Detect and respond to security threats by using Azure Sentinel

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](https://azure.microsoft.com/services/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.

## 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.

1. 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.

**Store and manage secrets by using Azure Key Vault**

[Azure Key Vault](https://azure.microsoft.com/services/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.

## 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.

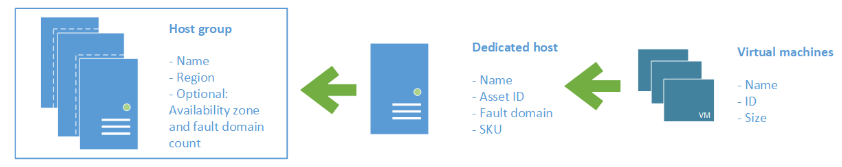
* **Simplified administration of application secrets**

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.

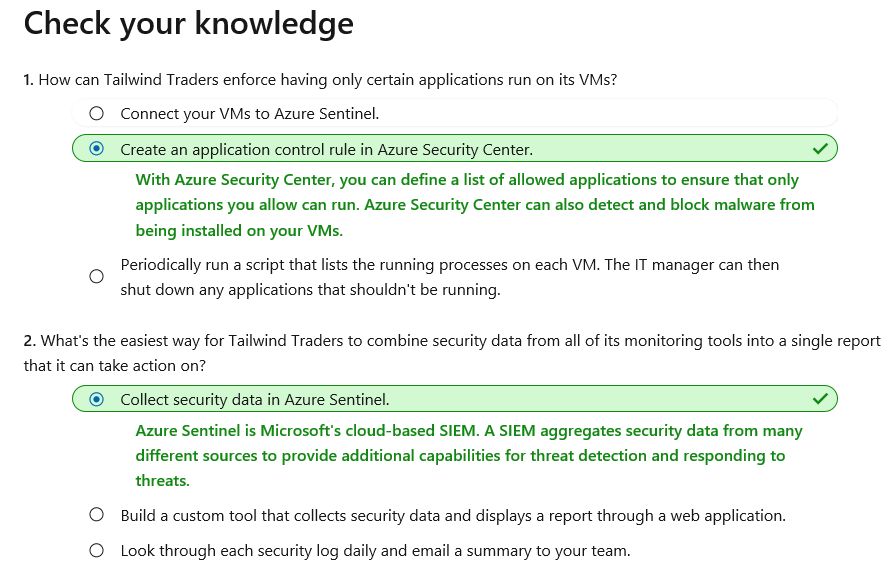
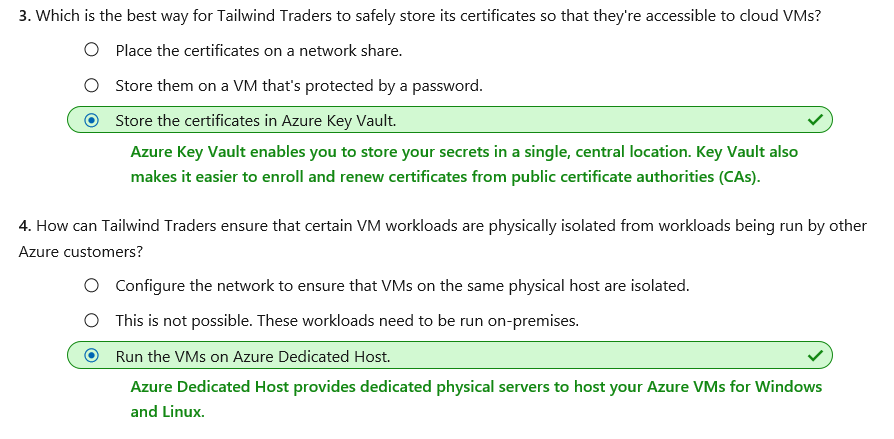
Here's a diagram that shows how virtual machines relate to dedicated hosts and host groups. A dedicated host is mapped to a physical server in an Azure datacenter. A host group is a collection of dedicated hosts.



## 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.
* Let’s you choose the number of processors, server capabilities, VM series, and VM sizes within the same host.

* Azure Security Center provides visibility of your security posture across all of your services, both on Azure and on-premises.
* Azure Sentinel aggregates security data from many different sources and provides additional capabilities for threat detection and response.
* Azure Key Vault stores your applications' secrets, such as passwords, encryption keys, and certificates, in a single, central location.
* Azure Dedicated Host provides dedicated physical servers to host your Azure VMs for Windows and Linux.

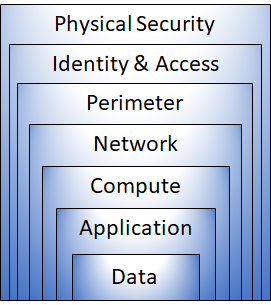
Module 4: Secure network connectivity

What is defense in depth?

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.

## 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.

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**
* **Integrity**
* **Availability**

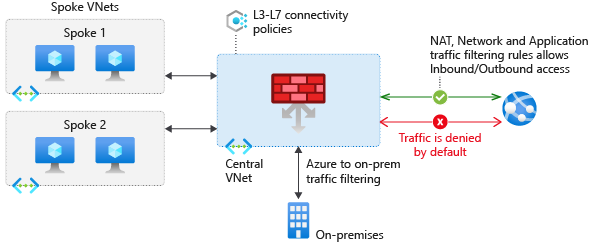
Protect virtual networks by using Azure Firewall

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.

## What's Azure Firewall?

[Azure Firewall](https://azure.microsoft.com/services/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:

[](https://docs.microsoft.com/en-us/learn/azure-fundamentals/secure-network-connectivity-azure/media/3-firewall-overview-large.png#lightbox)

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 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.

## 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](https://azure.microsoft.com/services/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](https://azure.microsoft.com/services/frontdoor/?) and [Azure Content Delivery Network](https://azure.microsoft.com/services/cdn/?) also provide WAF services.

Protect from DDoS attacks by using Azure DDoS Protection

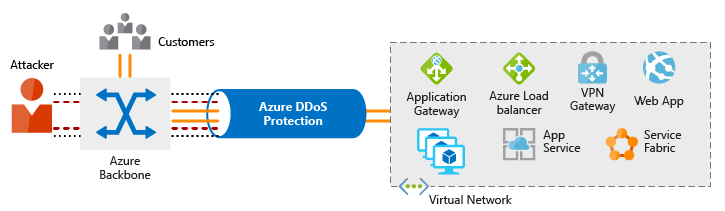
## What are DDoS attacks?

A [distributed denial of service](https://azure.microsoft.com/services/ddos-protection?) 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](https://azure.microsoft.com/services/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: 

## 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.

Filter network traffic by using network security groups

## What are network security groups?

A [network security group](https://docs.microsoft.com/en-us/azure/virtual-network/security-overview?#network-security-groups?azure-portal=true) 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.

## 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.

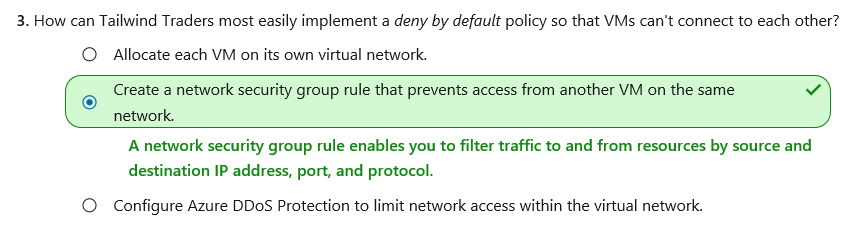
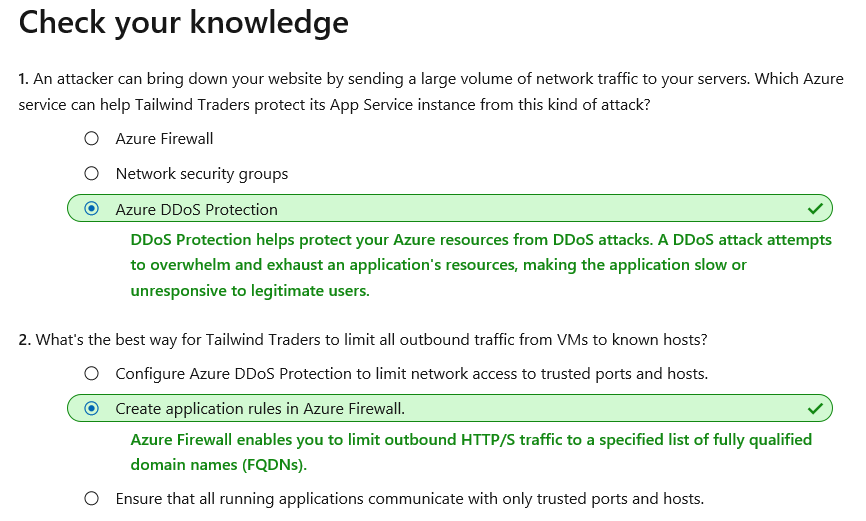
* **Azure Application Gateway web application firewall and Azure Firewall**

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.



Tailwind Traders now has a few tools and services that it can use to secure its networks. Here's a brief summary:

* Azure Firewall is a managed, cloud-based network security service that helps protect resources in Azure virtual networks.
* An Azure virtual network is similar to a traditional network that you'd operate in your own datacenter. It enables virtual machines and other compute resources to securely communicate with each other, the internet, and on-premises networks.
* A network security group (NSG) enables you to filter network traffic to and from Azure resources within a virtual network.
* Azure DDoS Protection helps protect Azure resources from DDoS attacks.

Module 3: Identify your product options

## 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

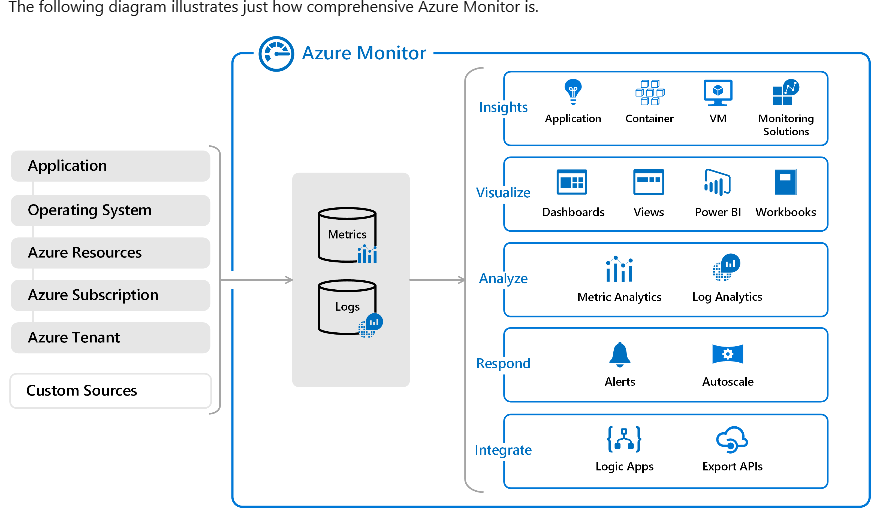
[Azure Advisor](https://azure.microsoft.com/services/advisor/?) evaluates your Azure resources and makes recommendations to help improve reliability, security, and performance, achieve operational excellence, and reduce costs. Advisor is designed to help you save time on cloud optimization. The recommendation service includes suggested actions you can take right away, postpone, or dismiss.

The recommendations are 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](https://azure.microsoft.com/services/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.



### Azure Service Health

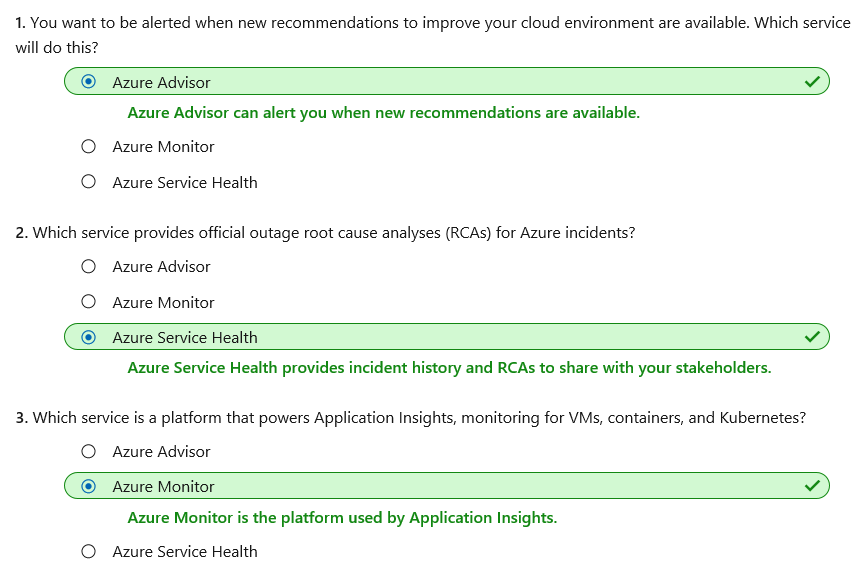
[Azure Service Health](https://azure.microsoft.com/features/service-health/?) provides a personalized view of the health of the Azure services, regions, and resources you rely on. The status.azure.com website, which displays only major issues that broadly affect Azure customers, doesn't provide the full 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.

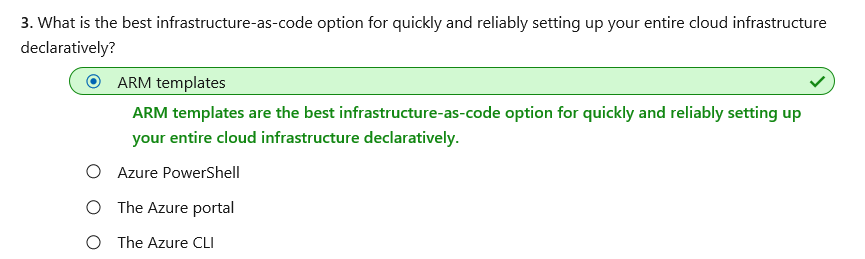
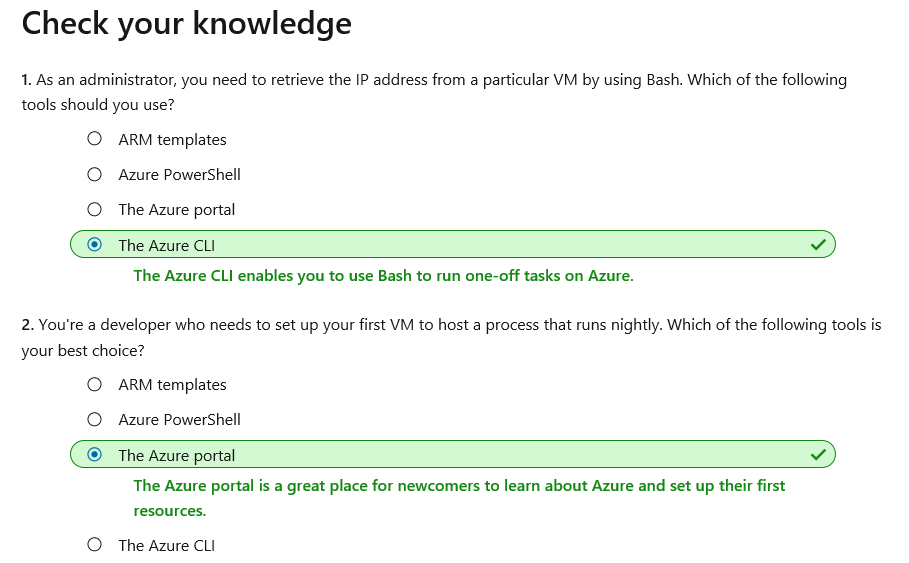
Service Health helps you keep an eye on several event types:

* **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.

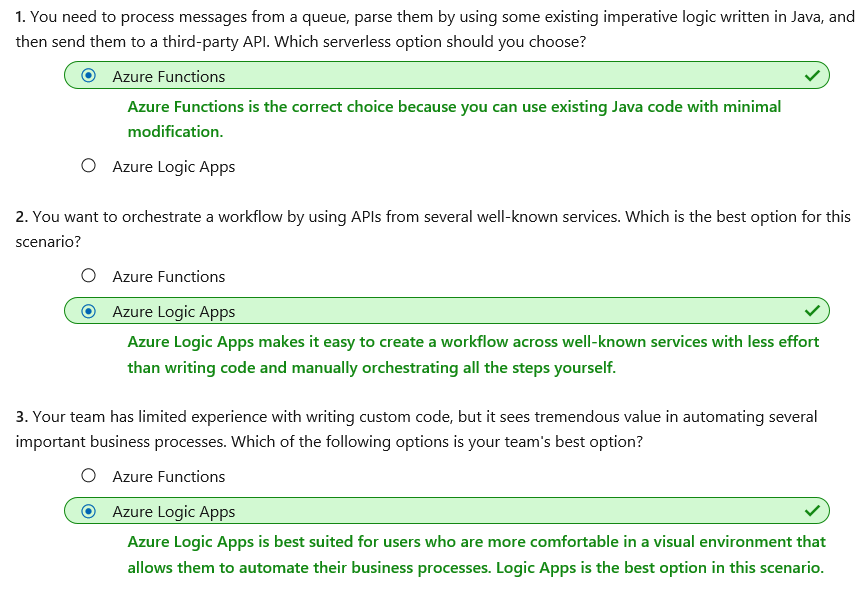
Azure Advisor is the right product option to help Tailwind Traders better understand and optimize both its cloud spend and its cloud security posture. This product might help the organization with other areas of its cloud usage as well.

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.





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.



## Azure IoT Hub

[Azure IoT Hub](https://azure.microsoft.com/services/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](https://azure.microsoft.com/services/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.

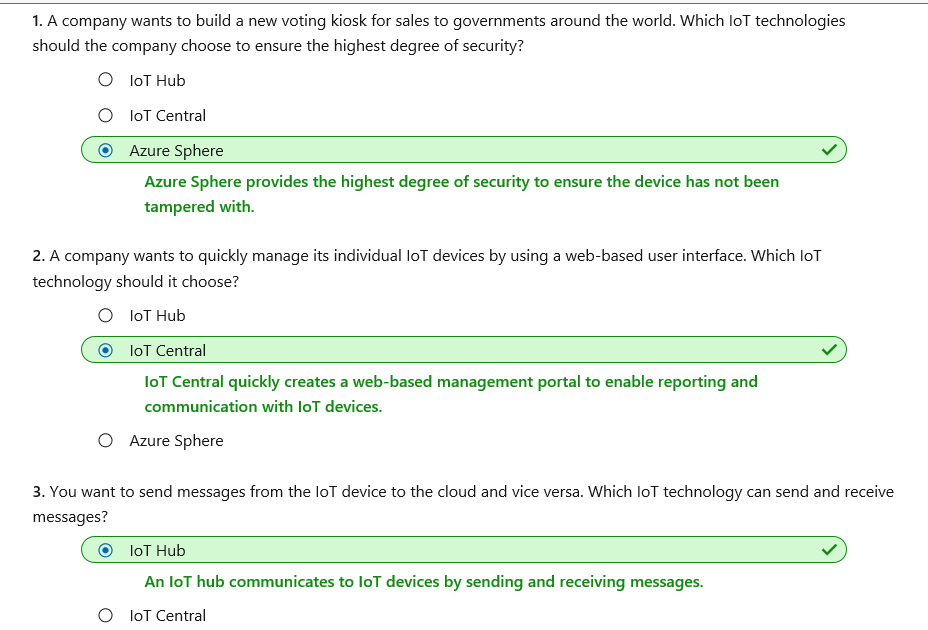
## Azure Sphere

[Azure Sphere](https://azure.microsoft.com/services/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 Seeed 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.



Compare authentication and authorization

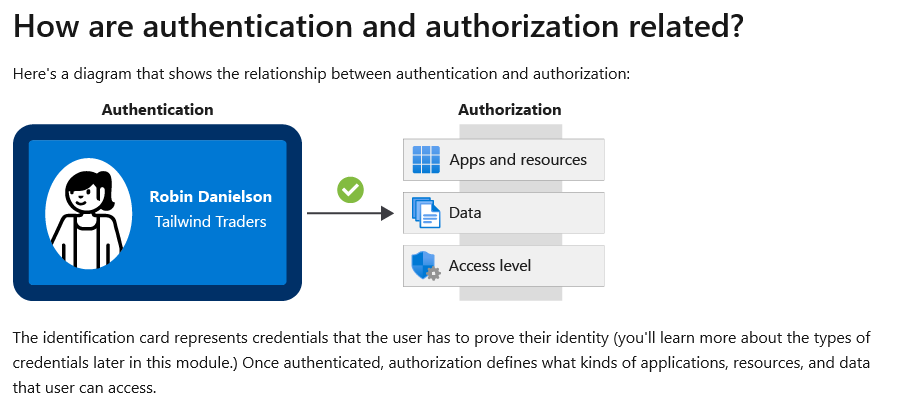
Two fundamental concepts that you need to understand when talking about identity and access are authentication (AuthN) and authorization (AuthZ).

## 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 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.

## 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'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.

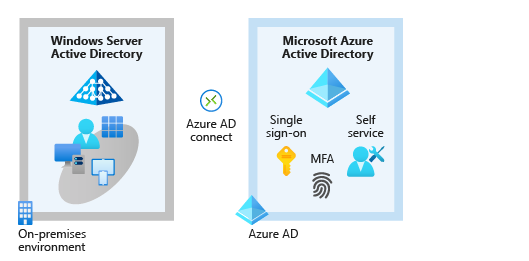
## How can I connect Active Directory with Azure AD?

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:



## 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.

## 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.

## What's Conditional Access?

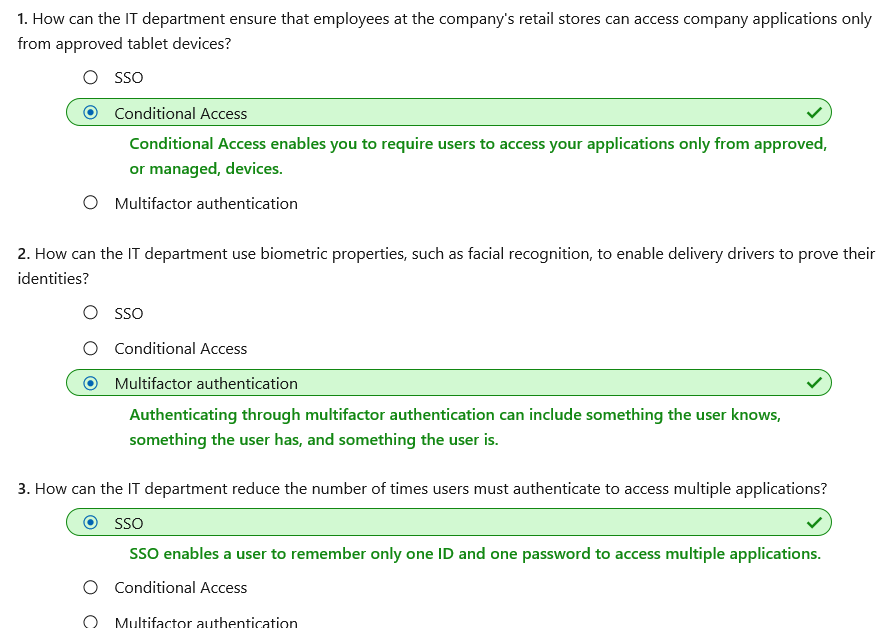
Conditional Access is a tool that Azure Active Directory uses to allow (or deny) access to resources based on identity signals. These signals include who the user is, where the user is, and what device the user is requesting access from.

Conditional Access helps IT administrators:

* Empower users to be productive wherever and whenever.
* Protect the organization's assets.

### 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.



Build a cloud governance strategy on Azure

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.

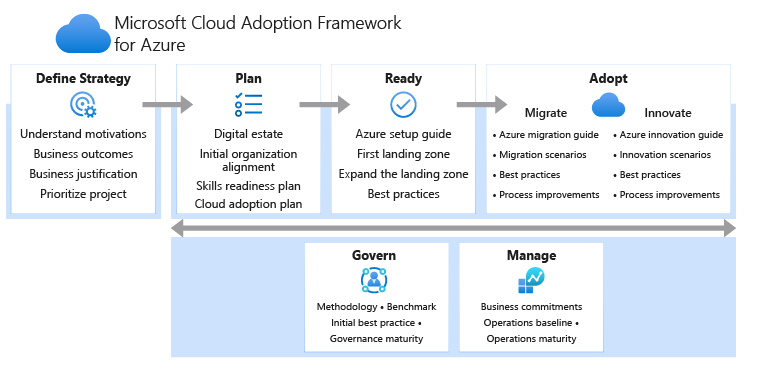
Accelerate cloud adoption journey by using the Cloud Adoption Framework for Azure

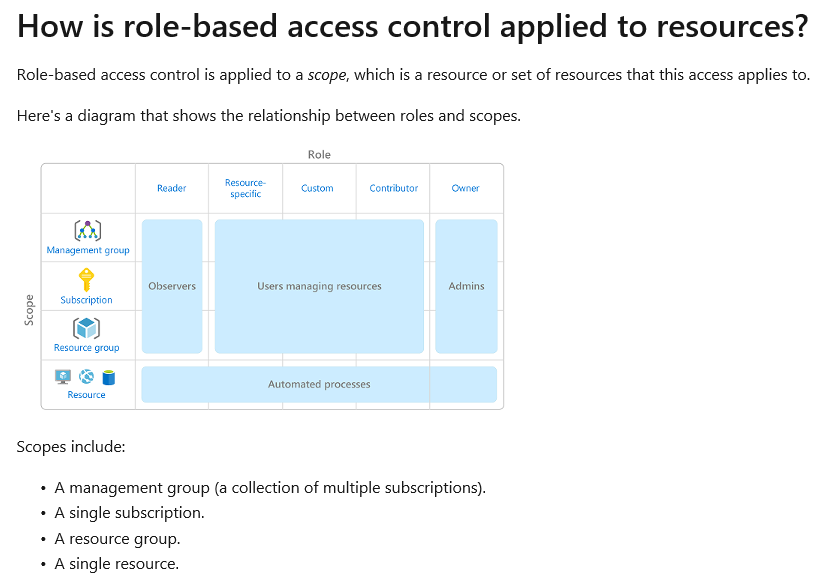
The [Cloud Adoption Framework for Azure](https://docs.microsoft.com/en-us/azure/cloud-adoption-framework/?) provides you with proven guidance to help with your cloud adoption journey. The Cloud Adoption Framework helps you create and implement the business and technology strategies needed to succeed in the cloud.

## 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.





## When should I use Azure RBAC?

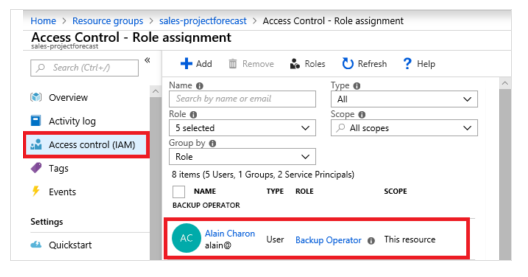
Use Azure RBAC when you need to:

* 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.

## 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.



# Prevent accidental changes by using resource locks

A [resource lock](https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/lock-resources?) prevents resources from being accidentally deleted or changed.

## 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.

Organize your Azure resources by using tags

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.

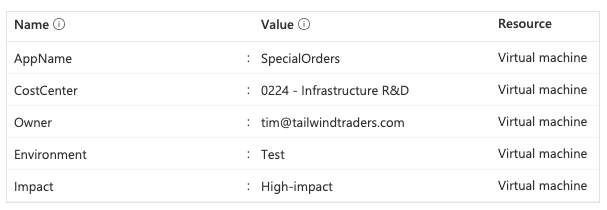
## How do I manage resource tags?

You can add, modify, or delete resource tags through PowerShell, the Azure CLI, Azure Resource Manager templates, the REST API, or the Azure portal

## 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.

Here's an example that shows these tags as they're applied to a virtual machine during provisioning.



Control and audit your resources by using Azure Policy

[Azure Policy](https://azure.microsoft.com/services/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.

## 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.

## 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.

# Exercise - Restrict deployments to a specific location by using Azure Policy

Completed 100 XP

* 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.

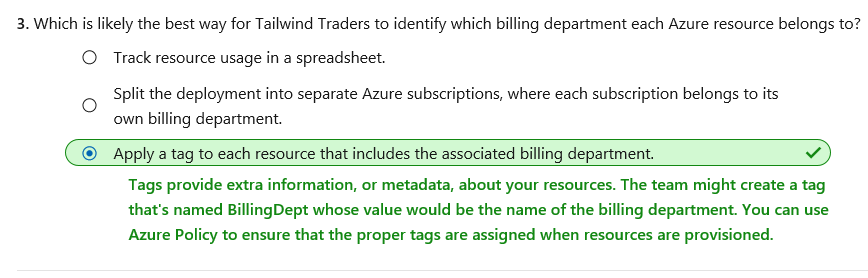
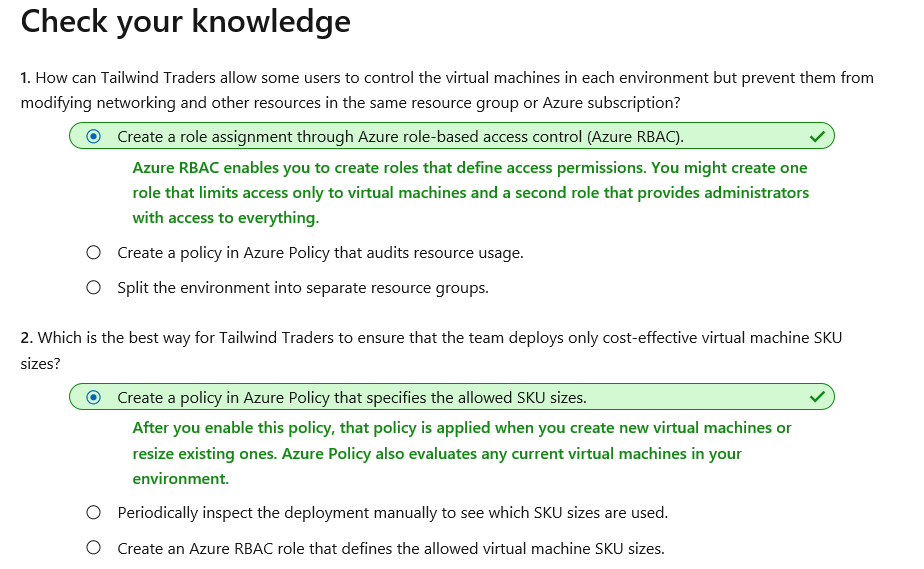
Tailwind Traders wants to limit the location where resources can be deployed to the **East US** region. It has two reasons:

* **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.



**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.

## What's in the Microsoft Privacy Statement?

The [Microsoft Privacy Statement](https://privacy.microsoft.com/privacystatement?) 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.

## What's in the Online Services Terms?

The [Online Services Terms](https://www.microsoft.com/licensing/terms/product/ForallOnlineServices?) (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.

Explore the Trust Center

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.

## What is the Azure compliance documentation?

The [Azure compliance documentation](https://docs.microsoft.com/en-us/azure/compliance/?) 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

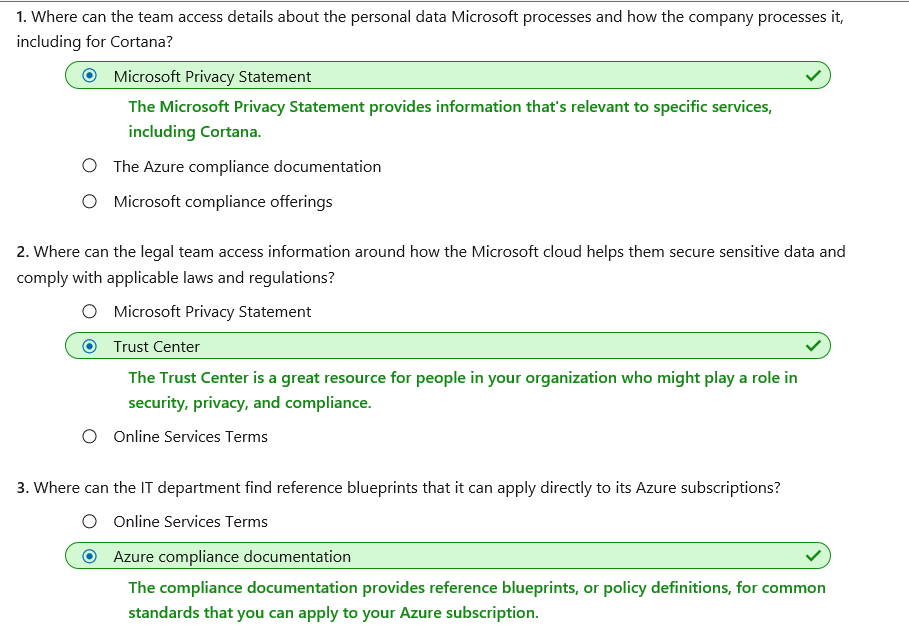
# What is Azure Government?

[Azure Government](https://azure.microsoft.com/global-infrastructure/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.

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.

What is Azure China 21Vianet?

[Azure China 21Vianet](https://docs.microsoft.com/en-us/azure/china?) 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.



# Summary

In this module, you learned about Microsoft's approach to privacy, security, and compliance. You explored resources specific to online services, including Azure, and how governments can use Azure to meet their specific security and compliance needs.

The security team at Tailwind Traders now has a better understanding of what resources are available to help it protect its data in the cloud and stay compliant:

* The [Microsoft Privacy Statement](https://privacy.microsoft.com/privacystatement?) provides trust in how Microsoft collects, protects, and uses customer data.
* The [Trust Center](https://www.microsoft.com/trustcenter?) provides you with documentation about compliance standards and how Azure can support your business.
* The [Azure compliance documentation](https://docs.microsoft.com/en-us/azure/compliance/?) includes detailed information about legal and regulatory standards and compliance on Azure.

Keep in mind that compliance status for Azure products and services doesn't automatically translate to compliance for the service or application you build or host on Azure. You're responsible for ensuring that you achieve compliance with the legal and regulatory standards that you must follow.