Azure Fundamentals

Contents

[Describe cloud Concepts 3](#_Toc180007201)

[Describe cloud computing 3](#_Toc180007202)

[Introduction to Microsoft Azure Fundamentals 3](#_Toc180007203)

[Introduction to cloud computing 4](#_Toc180007204)

[What is cloud computing 4](#_Toc180007205)

[Describe the shared responsibility model. 5](#_Toc180007206)

[Define cloud models. 7](#_Toc180007207)

[Describe the consumption-based model 8](#_Toc180007208)

[Knowledge check 10](#_Toc180007209)

[Summary 10](#_Toc180007210)

[Describe the benefits of using cloud services 12](#_Toc180007211)

[Introduction 12](#_Toc180007212)

[Describe the benefits of high availability and scalability in the cloud 12](#_Toc180007213)

[Describe the benefits of reliability and predictability in the cloud 13](#_Toc180007214)

[Describe the benefits of security and governance in the cloud 14](#_Toc180007215)

[Describe the benefits of manageability in the cloud 15](#_Toc180007216)

[Knowledge check 16](#_Toc180007217)

[Summary 16](#_Toc180007218)

[Describe cloud service types 17](#_Toc180007219)

[Introduction 17](#_Toc180007220)

[Describe Infrastructure as a Service 17](#_Toc180007221)

[Describe Platform as a Service 18](#_Toc180007222)

[Describe Software as a Service 19](#_Toc180007223)

[Knowledge check 20](#_Toc180007224)

[Summary 20](#_Toc180007225)

# Describe cloud Concepts

## Describe cloud computing

### Introduction to Microsoft Azure Fundamentals

Microsoft Azure is a cloud computing platform with an ever-expanding set of services to help you build solutions to meet your business goals. Azure services support everything from simple to complex. Azure has simple web services for hosting your business presence in the cloud. Azure also supports running fully virtualized computers managing your custom software solutions. Azure provides a wealth of cloud-based services like remote storage, database hosting, and centralized account management. Azure also offers new capabilities like artificial intelligence (AI) and Internet of Things (IoT) focused service

In this series, you’ll cover cloud computing basics, be introduced to some of the core services provided by Microsoft Azure and will learn more about the governance and compliance services that you can use.

#### What are Azure Fundamentals?

Azure Fundamentals is a series of three learning paths that familiarize you with Azure and its many services and features.

Whether you're interested in compute, networking, or storage services; learning about cloud security best practices; or exploring governance and management options, think of Azure Fundamentals as your curated guide to Azure.

Azure Fundamentals includes interactive exercises that give you hands-on experience with Azure. Many exercises provide a temporary Azure portal environment called the sandbox, which allows you to practice creating cloud resources for free at your own pace.

Technical IT experience isn't required; however, having general IT knowledge will help you get the most from your learning experience.

#### Why should I take Azure Fundamentals?

If you're just beginning to work with the cloud, or if you already have cloud experience, Azure Fundamentals provides you with everything you need to get started.

No matter your goals, Azure Fundamentals has something for you. You should take this course if you:

* Have general interest in Azure or in cloud computing
* Want to earn official certification from Microsoft (AZ-900)

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

|  |  |
| --- | --- |
| **AZ-900 Domain Area** | **Weight** |
| Describe cloud concepts | 25-30% |
| Describe Azure architecture and services | 35-40% |
| Describe Azure management and governance | 30-35% |

Each domain area maps to a learning path in Azure Fundamentals. The percentages shown indicate the relative weight of each area on the exam. The higher the percentage, the more questions that part of the exam will contain. Be sure to read the exam page for specifics about what skills are covered in each area.

This training helps you develop a broad understanding of Azure.

### Introduction to cloud computing

In this module, you’ll be introduced to general cloud concepts. You’ll start with an introduction to the cloud in general. Then you'll dive into concepts like shared responsibility, different cloud models, and explore the unique pricing method for the cloud.

If you are already familiar with cloud computing, this module may be largely review for you.

#### Learning objectives

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

* Define cloud computing.
* Describe the shared responsibility model.
* Define cloud models, including public, private, and hybrid.
* Identify appropriate use cases for each cloud model.
* Describe the consumption-based model.
* Compare cloud pricing models.

### What is cloud computing

Cloud computing is the delivery of computing services over the internet. Computing services include common IT infrastructure such as virtual machines, storage, databases, and networking. Cloud services also expand the traditional IT offerings to include things like Internet of Things (IoT), machine learning (ML), and artificial intelligence (AI).

Because cloud computing uses the internet to deliver these services, it doesn’t have to be constrained by physical infrastructure the same way that a traditional datacenter is. That means if you need to increase your IT infrastructure rapidly, you don’t have to wait to build a new datacenter—you can use the cloud to rapidly expand your IT footprint.

[This short video provides a quick introduction to cloud computing.](https://www.microsoft.com/en-us/videoplayer/embed/RE4LyBB?postJsllMsg=true)

### Describe the shared responsibility model.

You may have heard of the shared responsibility model, but you may not understand what it means or how it impacts cloud computing.

Start with a traditional corporate datacenter. The company is responsible for maintaining the physical space, ensuring security, and maintaining or replacing the servers if anything happens. The IT department is responsible for maintaining all the infrastructure and software needed to keep the datacenter up and running. They’re also likely to be responsible for keeping all systems patched and on the correct version.

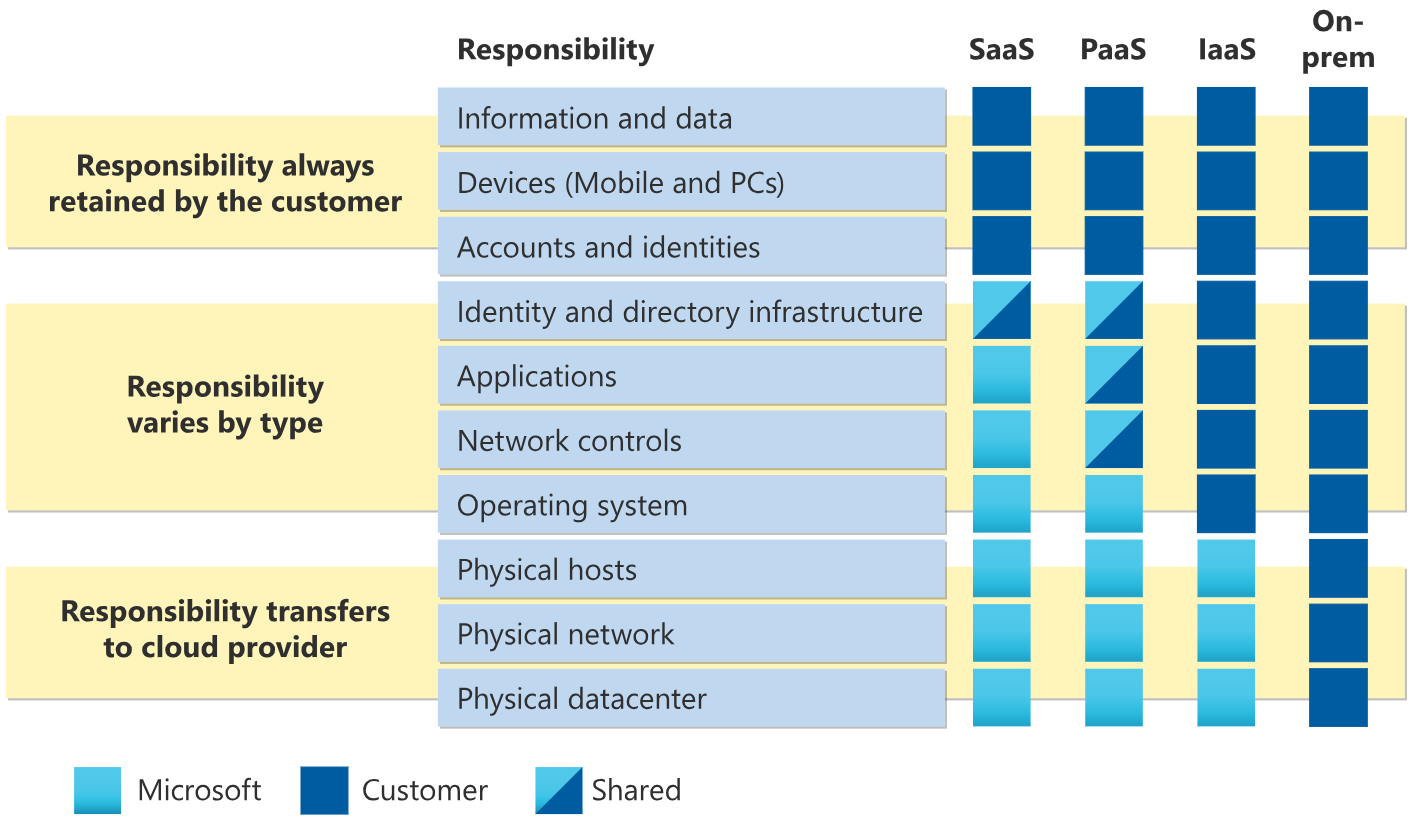
With the shared responsibility model, these responsibilities get shared between the cloud provider and the consumer. Physical security, power, cooling, and network connectivity are the responsibility of the cloud provider. The consumer isn’t collocated with the datacenter, so it wouldn’t make sense for the consumer to have any of those responsibilities.

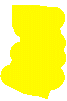
At the same time, the consumer is responsible for the data and information stored in the cloud. (You wouldn’t want the cloud provider to be able to read your information.) The consumer is also responsible for access security, meaning you only give access to those who need it.

Then, for some things, the responsibility depends on the situation. If you’re using a cloud SQL database, the cloud provider would be responsible for maintaining the actual database. However, you’re still responsible for the data that gets ingested into the database. If you deployed a virtual machine and installed an SQL database on it, you’d be responsible for database patches and updates, as well as maintaining the data and information stored in the database.

With an on-premises datacenter, you’re responsible for everything. With cloud computing, those responsibilities shift. The shared responsibility model is heavily tied into the cloud service types (covered later in this learning path): infrastructure as a service (IaaS), platform as a service (PaaS), and software as a service (SaaS). IaaS places the most responsibility on the consumer, with the cloud provider being responsible for the basics of physical security, power, and connectivity. On the other end of the spectrum, SaaS places most of the responsibility with the cloud provider. PaaS, being a middle ground between IaaS and SaaS, rests somewhere in the middle and evenly distributes responsibility between the cloud provider and the consumer.

The following diagram highlights how the Shared Responsibility Model informs who is responsible for what, depending on the cloud service type.





When using a cloud provider, you’ll always be responsible for:

* The information and data stored in the cloud
* Devices that are allowed to connect to your cloud (cell phones, computers, and so on)
* The accounts and identities of the people, services, and devices within your organization

The cloud provider is always responsible for:

* The physical datacenter
* The physical network
* The physical hosts

Your service model will determine responsibility for things like:

* Operating systems
* Network controls
* Applications
* Identity and infrastructure

### Define cloud models.

What are cloud models? The cloud models define the deployment type of cloud resources. The three main cloud models are: private, public, and hybrid.

#### Private cloud

Let us start with a private cloud. A private cloud is, in some ways, the natural evolution from a corporate datacenter. It’s a cloud (delivering IT services over the internet) that’s used by a single entity. Private cloud provides much greater control for the company and its IT department. However, it also comes with greater cost and fewer of the benefits of a public cloud deployment. Finally, a private cloud may be hosted from your on-site datacenter. It may also be hosted in a dedicated datacenter offsite, potentially even by a third party that has dedicated that datacenter to your company.

#### Public cloud

A public cloud is built, controlled, and maintained by a third-party cloud provider. With a public cloud, anyone that wants to purchase cloud services can access and use resources. The general public availability is a key difference between public and private clouds.

#### Hybrid cloud

A hybrid cloud is a computing environment that uses both public and private clouds in an inter-connected environment. A hybrid cloud environment can be used to allow a private cloud to surge for increased, temporary demand by deploying public cloud resources. Hybrid cloud can be used to provide an extra layer of security. For example, users can flexibly choose which services to keep in public cloud and which to deploy to their private cloud infrastructure.

The following table highlights a few key comparative aspects between the cloud models.

|  |  |  |
| --- | --- | --- |
| **Public cloud** | **Private cloud** | **Hybrid cloud** |
| No capital expenditures to scale up | Organizations have complete control over resources and security | Provides the most flexibility |
| Organizations pay only for what they use | Hardware must be purchased for startup and maintenance | Organizations control security, compliance, or legal requirements |
| Organizations don’t have complete control over resources and security | Organizations are responsible for hardware maintenance and updates |  |
| Applications can be quickly provisioned and deprovisioned | Data is not collocated with other organizations’ data | Organizations determine where to run their applications |

#### Multi-cloud

A fourth, and increasingly likely scenario is a multi-cloud scenario. In a multi-cloud scenario, you use multiple public cloud providers. Maybe you use different features from different cloud providers. Or maybe you started your cloud journey with one provider and are in the process of migrating to a different provider. Regardless, in a multi-cloud environment you deal with two (or more) public cloud providers and manage resources and security in both environments.

#### Azure Arc

Azure Arc is a set of technologies that helps manage your cloud environment. Azure Arc can help manage your cloud environment, whether it's a public cloud solely on Azure, a private cloud in your datacenter, a hybrid configuration, or even a multi-cloud environment running on multiple cloud providers at once.

#### Azure VMware Solution

What if you’re already established with VMware in a private cloud environment but want to migrate to a public or hybrid cloud? Azure VMware Solution lets you run your VMware workloads in Azure with seamless integration and scalability.

### Describe the consumption-based model

When comparing IT infrastructure models, there are two types of expenses to consider. Capital expenditure (CapEx) and operational expenditure (OpEx).

CapEx is typically a one-time, up-front expenditure to purchase or secure tangible resources. A new building, repaving the parking lot, building a datacenter, or buying a company vehicle are examples of CapEx.

In contrast, OpEx is spending money on services or products over time. Renting a convention center, leasing a company vehicle, or signing up for cloud services are all examples of OpEx.

Cloud computing falls under OpEx because cloud computing operates on a consumption-based model. With cloud computing, you don’t pay for the physical infrastructure, the electricity, the security, or anything else associated with maintaining a datacenter. Instead, you pay for the IT resources you use. If you don’t use any IT resources this month, you don’t pay for any IT resources.

This consumption-based model has many benefits, including:

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

With a traditional datacenter, you try to estimate the future resource needs. If you overestimate, you spend more on your datacenter than you need to and potentially waste money. If you underestimate, your datacenter will quickly reach capacity and your applications and services may suffer from decreased performance. Fixing an under-provisioned datacenter can take a long time. You may need to order, receive, and install more hardware. You'll also need to add power, cooling, and networking for the extra hardware.

In a cloud-based model, you don’t have to worry about getting the resource needs just right. If you find that you need more virtual machines, you add more. If the demand drops and you don’t need as many virtual machines, you remove machines as needed. Either way, you’re only paying for the virtual machines that you use, not the “extra capacity” that the cloud provider has on hand.

#### Compare cloud pricing models

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

* Plan and manage your operating costs.
* Run your infrastructure more efficiently.
* Scale as your business needs change.

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

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

### [Knowledge check](https://learn.microsoft.com/en-us/training/modules/describe-cloud-compute/7-knowledge-check)

### Summary

In this module, you learned about general cloud concepts. You started with things like just understanding what cloud computing is. You also learned about the shared responsibility model and how you and your cloud provider share the responsibility of keeping your information in the cloud secure. You briefly covered the differences between the cloud models (public, private, hybrid, and multi-cloud). Then, you wrapped up with a unit on how the cloud shifts IT spend from a capital expense to an operational expense.

#### Learning objectives

You should now be able to:

* Define cloud computing.
* Describe the shared responsibility model.
* Define cloud models, including public, private, and hybrid.
* Identify appropriate use cases for each cloud model.
* Describe the consumption-based model.
* Compare cloud pricing models.

#### Additional resources

The following resources provide more information on topics in this module or related to this module.

* [Shared responsibility model](https://learn.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility) - The shared responsibility model is the sharing of responsibilities for the cloud between you and your cloud provider.
* [Introduction to Azure VMware Solution](https://learn.microsoft.com/en-us/learn/modules/intro-azure-vmware-solution/) is a Microsoft Learn course that dives deeper into Azure VMware Solution.
* [Introduction to Azure hybrid cloud services](https://learn.microsoft.com/en-us/learn/modules/intro-to-azure-hybrid-services/) is a Microsoft Learn course that explains hybrid cloud in greater detail.

## Describe the benefits of using cloud services

### Introduction

In this module, you’ll be introduced to some of the benefits that cloud computing offers. You’ll learn how cloud computing can help you meet variable demand while providing a good experience for your customer. You’ll also learn about security, governance, and overall manageability in the cloud.

#### Learning objectives

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

* Describe the benefits of high availability and scalability in the cloud.
* Describe the benefits of reliability and predictability in the cloud.
* Describe the benefits of security and governance in the cloud.
* Describe the benefits of manageability in the cloud.

### Describe the benefits of high availability and scalability in the cloud

When building or deploying a cloud application, two of the biggest considerations are uptime (or availability) and the ability to handle demand (or scale).

#### High availability

When you’re deploying an application, a service, or any IT resources, it’s important the resources are available when needed. High availability focuses on ensuring maximum availability, regardless of disruptions or events that may occur.

When you’re architecting your solution, you’ll need to account for service availability guarantees. Azure is a highly available cloud environment with uptime guarantees depending on the service. These guarantees are part of the service-level agreements (SLAs).

[This short video describes Azure SLAs in more detail.](https://www.microsoft.com/en-us/videoplayer/embed/RWEA4z?postJsllMsg=true)

#### Scalability

Another major benefit of cloud computing is the scalability of cloud resources. Scalability refers to the ability to adjust resources to meet demand. If you suddenly experience peak traffic and your systems are overwhelmed, the ability to scale means you can add more resources to better handle the increased demand.

The other benefit of scalability is that you aren't overpaying for services. Because the cloud is a consumption-based model, you only pay for what you use. If demand drops off, you can reduce your resources and thereby reduce your costs.

Scaling generally comes in two varieties: vertical and horizontal. Vertical scaling is focused on increasing or decreasing the capabilities of resources. Horizontal scaling is adding or subtracting the number of resources.

##### Vertical scaling

With vertical scaling, if you were developing an app and you needed more processing power, you could vertically scale up to add more CPUs or RAM to the virtual machine. Conversely, if you realized you had over-specified the needs, you could vertically scale down by lowering the CPU or RAM specifications.

##### Horizontal scaling

With horizontal scaling, if you suddenly experienced a steep jump in demand, your deployed resources could be scaled out (either automatically or manually). For example, you could add additional virtual machines or containers, scaling out. In the same manner, if there was a significant drop in demand, deployed resources could be scaled in (either automatically or manually), scaling in.

### Describe the benefits of reliability and predictability in the cloud

Reliability and predictability are two crucial cloud benefits that help you develop solutions with confidence.

#### Reliability

Reliability is the ability of a system to recover from failures and continue to function. It's also one of the pillars of the Microsoft Azure Well-Architected Framework.

The cloud, by virtue of its decentralized design, naturally supports a reliable and resilient infrastructure. With a decentralized design, the cloud enables you to have resources deployed in regions around the world. With this global scale, even if one region has a catastrophic event other regions are still up and running. You can design your applications to automatically take advantage of this increased reliability. In some cases, your cloud environment itself will automatically shift to a different region for you, with no action needed on your part. You’ll learn more about how Azure leverages global scale to provide reliability later in this series.

#### Predictability

Predictability in the cloud lets you move forward with confidence. Predictability can be focused on performance predictability or cost predictability. Both performance and cost predictability are heavily influenced by the Microsoft Azure Well-Architected Framework. Deploy a solution built around this framework and you have a solution whose cost and performance are predictable.

##### Performance

Performance predictability focuses on predicting the resources needed to deliver a positive experience for your customers. Autoscaling, load balancing, and high availability are just some of the cloud concepts that support performance predictability. If you suddenly need more resources, autoscaling can deploy additional resources to meet the demand, and then scale back when the demand drops. Or if the traffic is heavily focused on one area, load balancing will help redirect some of the overload to less stressed areas.

##### Cost

Cost predictability is focused on predicting or forecasting the cost of the cloud spend. With the cloud, you can track your resource use in real time, monitor resources to ensure that you’re using them in the most efficient way, and apply data analytics to find patterns and trends that help better plan resource deployments. By operating in the cloud and using cloud analytics and information, you can predict future costs and adjust your resources as needed. You can even use tools like the Total Cost of Ownership (TCO) or Pricing Calculator to get an estimate of potential cloud spend.

### Describe the benefits of security and governance in the cloud

Whether you’re deploying infrastructure as a service or software as a service, cloud features support governance and compliance. Things like set templates help ensure that all your deployed resources meet corporate standards and government regulatory requirements. Plus, you can update all your deployed resources to new standards as standards change. Cloud-based auditing helps flag any resource that’s out of compliance with your corporate standards and provides mitigation strategies. Depending on your operating model, software patches and updates may also automatically be applied, which helps with both governance and security.

On the security side, you can find a cloud solution that matches your security needs. If you want maximum control of security, infrastructure as a service provides (IaaS) you with physical resources but lets you manage the operating systems and installed software, including patches and maintenance. If you want patches and maintenance taken care of automatically, platform as a service or software as a service deployment may be the best cloud strategies for you.

And because the cloud is intended as an over-the-internet delivery of IT resources, cloud providers are typically well suited to handle things like distributed denial of service (DDoS) attacks, making your network more robust and secure.

By establishing a good governance footprint early, you can keep your cloud footprint updated, secure, and well managed.

### Describe the benefits of manageability in the cloud

A major benefit of cloud computing is the manageability options. There are two types of manageability for cloud computing that you’ll learn about in this series, and both are excellent benefits.

#### Management of the cloud

Management of the cloud speaks to managing your cloud resources. In the cloud, you can:

* Automatically scale resource deployment based on need.
* Deploy resources based on a preconfigured template, removing the need for manual configuration.
* Monitor the health of resources and automatically replace failing resources.
* Receive automatic alerts based on configured metrics, so you’re aware of performance in real time.

#### Management in the cloud

Management in the cloud speaks to how you’re able to manage your cloud environment and resources. You can manage these:

* Through a web portal.
* Using a command line interface.
* Using APIs.
* Using PowerShell.

### [Knowledge check](https://learn.microsoft.com/en-us/training/modules/describe-benefits-use-cloud-services/6-knowledge-check)

### Summary

In this module, you learned about some of the benefits of operating in the cloud. You learned about high availability and reliability, and how those work to keep your applications running. You also learned about how the cloud can provide a more secure environment. Finally, you learned that the cloud provides a highly manageable environment for your resources.

#### Learning objectives

You should now be able to:

* Describe the benefits of high availability and scalability in the cloud.
* Describe the benefits of reliability and predictability in the cloud.
* Describe the benefits of security and governance in the cloud.
* Describe the benefits of manageability in the cloud.

#### Additional resources

The following resources provide more information on topics in this module or related to this module.

* [Build great solutions with the Microsoft Azure Well-Architected Framework](https://learn.microsoft.com/en-us/learn/paths/azure-well-architected-framework/) is a Microsoft Learn course that introduces you to the Microsoft Azure Well-Architected Framework.

## Describe cloud service types

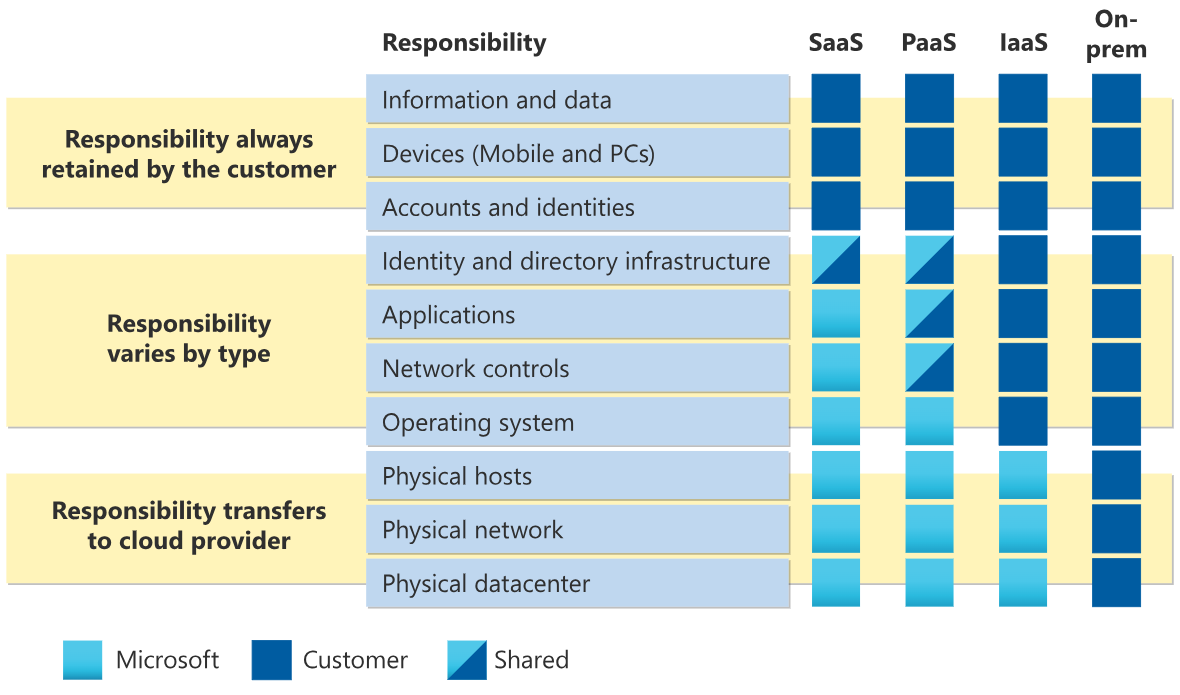
### Introduction

In this module, you’ll be introduced to cloud service types. You’ll learn how each cloud service type determines the flexibility you’ll have with managing and configuring resources. You'll understand how the shared responsibility model applies to each cloud service type, and about various use cases for each cloud service type.

#### Learning objectives

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

* Describe infrastructure as a service (IaaS).
* Describe platform as a service (PaaS).
* Describe software as a service (SaaS).
* Identify appropriate use cases for each cloud service (IaaS, PaaS, SaaS).



### Describe Infrastructure as a Service

Infrastructure as a service (IaaS) is the most flexible category of cloud services, as it provides you the maximum amount of control for your cloud resources. In an IaaS model, the cloud provider is responsible for maintaining the hardware, network connectivity (to the internet), and physical security. You’re responsible for everything else: operating system installation, configuration, and maintenance; network configuration; database and storage configuration; and so on. With IaaS, you’re essentially renting the hardware in a cloud datacenter, but what you do with that hardware is up to you.

#### Shared responsibility model

The shared responsibility model applies to all the cloud service types. IaaS places the largest share of responsibility with you. The cloud provider is responsible for maintaining the physical infrastructure and its access to the internet. You’re responsible for installation and configuration, patching and updates, and security.

#### Scenarios

Some common scenarios where IaaS might make sense include:

* Lift-and-shift migration: You’re setting up cloud resources similar to your on-prem datacenter, and then simply moving the things running on-prem to running on the IaaS infrastructure.
* Testing and development: You have established configurations for development and test environments that you need to rapidly replicate. You can start up or shut down the different environments rapidly with an IaaS structure, while maintaining complete control.

### Describe Platform as a Service

Platform as a service (PaaS) is a middle ground between renting space in a datacenter (infrastructure as a service) and paying for a complete and deployed solution (software as a service). In a PaaS environment, the cloud provider maintains the physical infrastructure, physical security, and connection to the internet. They also maintain the operating systems, middleware, development tools, and business intelligence services that make up a cloud solution. In a PaaS scenario, you don't have to worry about the licensing or patching for operating systems and databases.

PaaS is well suited to provide a complete development environment without the headache of maintaining all the development infrastructure.

#### Shared responsibility model

The shared responsibility model applies to all the cloud service types. PaaS splits the responsibility between you and the cloud provider. The cloud provider is responsible for maintaining the physical infrastructure and its access to the internet, just like in IaaS. In the PaaS model, the cloud provider will also maintain the operating systems, databases, and development tools. Think of PaaS like using a domain joined machine: IT maintains the device with regular updates, patches, and refreshes.

Depending on the configuration, you or the cloud provider may be responsible for networking settings and connectivity within your cloud environment, network and application security, and the directory infrastructure.

#### Scenarios

Some common scenarios where PaaS might make sense include:

* Development framework: PaaS provides a framework that developers can build upon to develop or customize cloud-based applications. Similar to the way you create an Excel macro, PaaS lets developers create applications using built-in software components. Cloud features such as scalability, high-availability, and multi-tenant capability are included, reducing the amount of coding that developers must do.
* Analytics or business intelligence: Tools provided as a service with PaaS allow organizations to analyze and mine their data, finding insights and patterns and predicting outcomes to improve forecasting, product design decisions, investment returns, and other business decisions.

### Describe Software as a Service

Software as a service (SaaS) is the most complete cloud service model from a product perspective. With SaaS, you’re essentially renting or using a fully developed application. Email, financial software, messaging applications, and connectivity software are all common examples of a SaaS implementation.

While the SaaS model may be the least flexible, it’s also the easiest to get up and running. It requires the least amount of technical knowledge or expertise to fully employ.

#### Shared responsibility model

The shared responsibility model applies to all the cloud service types. SaaS is the model that places the most responsibility with the cloud provider and the least responsibility with the user. In a SaaS environment you’re responsible for the data that you put into the system, the devices that you allow to connect to the system, and the users that have access. Nearly everything else falls to the cloud provider. The cloud provider is responsible for physical security of the datacenters, power, network connectivity, and application development and patching.

#### Scenarios

Some common scenarios for SaaS are:

* Email and messaging.
* Business productivity applications.
* Finance and expense tracking.

### [Knowledge check](https://learn.microsoft.com/en-us/training/modules/describe-cloud-service-types/5-knowledge-check)

### Summary

In this module, you learned about the cloud service types and some common scenarios for each type. You also reinforced how the shared responsibility model determines your responsibilities with different cloud service types.

#### Learning objectives

You should now be able to:

* Describe infrastructure as a service (IaaS).
* Describe platform as a service (PaaS).
* Describe software as a service (SaaS).
* Identify appropriate use cases for each cloud service (IaaS, PaaS, SaaS).

# Describe Azure architecture and services

## Describe the core architectural components of Azure

### Introduction

In this module, you’ll be introduced to the core architectural components of Azure. You’ll learn about the physical organization of Azure: datacenters, availability zones, and regions; and you’ll learn about the organizational structure of Azure: resources and resource groups, subscriptions, and management groups.

#### Learning objectives

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

* Describe Azure regions, region pairs, and sovereign regions.
* Describe Availability Zones.
* Describe Azure datacenters.
* Describe Azure resources and Resource Groups.
* Describe subscriptions.
* Describe management groups.
* Describe the hierarchy of resource groups, subscriptions, and management groups.

### What is Microsoft Azure

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

[This short video provides the information of what is Microsoft Azure](https://www.microsoft.com/en-us/videoplayer/embed/RWEsag?postJsllMsg=true)

#### What does Azure offer?

**Limitless innovation.** Build intelligent apps and solutions with advanced technology, tools, and services to take your business to the next level. Seamlessly unify your technology to simplify platform management and to deliver innovations efficiently and securely on a trusted cloud.

* **Bring ideas to life:** Build on a trusted platform to advance your organization with industry-leading AI and cloud services.
* **Seamlessly unify:** Efficiently manage all your infrastructure, data, analytics, and AI solutions across an integrated platform.
* **Innovate on trust:** Rely on trusted technology from a partner who's dedicated to security and responsibility.

#### What can I do with Azure?

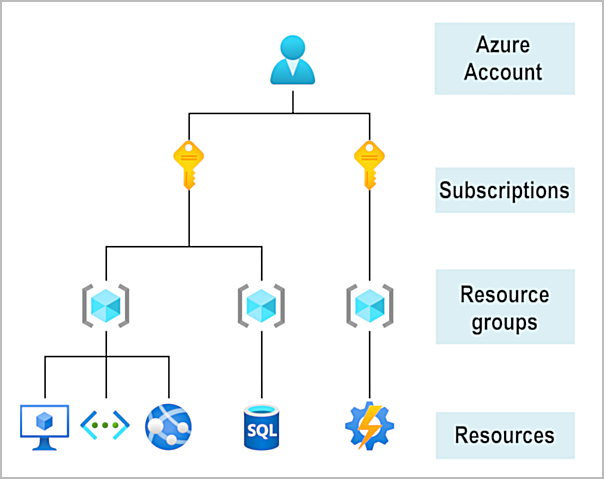
Azure provides more than 100 services that enable you to do everything from running your existing applications on virtual machines to exploring new software paradigms, such as intelligent bots and mixed reality.

Many teams start exploring the cloud by moving their existing applications to virtual machines (VMs) that run in Azure. Migrating your existing apps to VMs is a good start, but the cloud is much more than a different place to run your VMs.

For example, Azure provides artificial intelligence (AI) and machine-learning (ML) services that can naturally communicate with your users through vision, hearing, and speech. It also provides storage solutions that dynamically grow to accommodate massive amounts of data. Azure services enable solutions that aren't feasible without the power of the cloud.

### Get started with Azure accounts

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



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

#### Create an Azure account

You can purchase Azure access directly from Microsoft by signing up on the Azure website or through a Microsoft representative. You can also purchase Azure access through a Microsoft partner. Cloud Solution Provider partners offer a range of complete managed-cloud solutions for Azure.

[Video on create an Azure account](https://learn.microsoft.com/en-us/training/modules/describe-core-architectural-components-of-azure/3-get-started-azure-accounts)

#### What is the Azure free account?

The Azure free account includes:

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

The [Azure free account](https://azure.microsoft.com/free) 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 Azure free student account?

The Azure free student account offer includes:

* Free access to certain Azure services for 12 months.
* A credit to use in the first 12 months.
* Free access to certain software developer tools.

The [Azure free student account](https://azure.microsoft.com/free/students/) is an offer for students that gives $100 credit and free developer tools. Also, you can sign up without a credit card.

#### What is the Microsoft 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 during 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. However, the sandbox is the preferred method to use because it allows you to create and test Azure resources at no cost to you.

### Exercise - Explore the Learn sandbox

In this exercise, you explore the Learn sandbox. You can interact with the Learn sandbox in three different ways. During exercises, you'll be provided for instructions for at least one of the methods below.

You start by activating the Learn sandbox. Then, you’ll investigate each of the methods to work in the Learn sandbox.

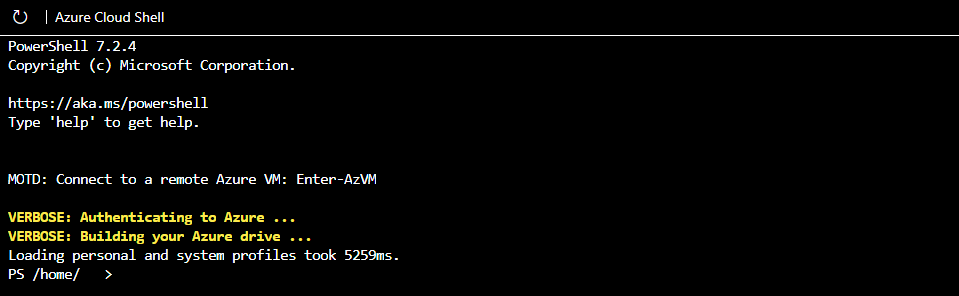
#### Activate the Learn Sandbox

If you haven’t already, use the Activate sandbox button above to activate the Learn sandbox.

If you receive a notice saying Microsoft Learn needs your permission to create Azure resource, use the Review permission button to review and accept the permissions. Once you approve the permissions, it may take a few minutes for the sandbox to activate.

#### Task 1: Use the PowerShell CLI

Once the sandbox launches, half the screen will be in PowerShell command line interface (CLI) mode. If you’re familiar with PowerShell, you can manage your Azure environment using PowerShell commands.



 Tip

You can tell you're in PowerShell mode by the PS before your directory on the command line.

Use the PowerShell Get-date command to get the current date and time.

PowerShell

Get-date

Most Azure specific commands will start with the letters az. The Get-date command you just ran is a PowerShell specific command. Let's try an Azure command to check what version of the CLI you're using right now.

PowerShell

az version

#### Task 2: Use the BASH CLI

If you’re more familiar with BASH, you can use BASH command instead by shifting to the BASH CLI.

Enter bash to switch to the BASH CLI.

PowerShell

bash



Tip

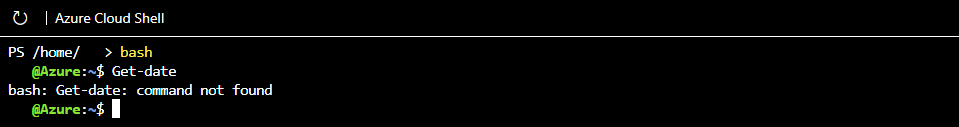
You can tell you're in BASH mode by the username displayed on the command line. It will be your username@azure.

Again, use the Get-date command to get the current date and time.

Azure CLI

Get-date

You received an error because Get-date is a PowerShell specific command.



Use the date command to get the current date and time.

Azure CLI

date

Just like in the PowerShell mode of the CLI, you can use the letters az to start an Azure command in the BASH mode. Try to run an update to the CLI with az upgrade.

Azure CLI

az upgrade

You can change back to PowerShell mode by entering pwsh on the BASH command line.

#### Task 3: Use Azure CLI interactive mode

Another way to interact is using the Azure CLI interactive mode. This changes CLI behavior to more closely resemble an integrated development environment (IDE). Interactive mode provides autocompletion, command descriptions, and even examples. If you’re unfamiliar with BASH and PowerShell, but want to use the command line, interactive mode may help you.

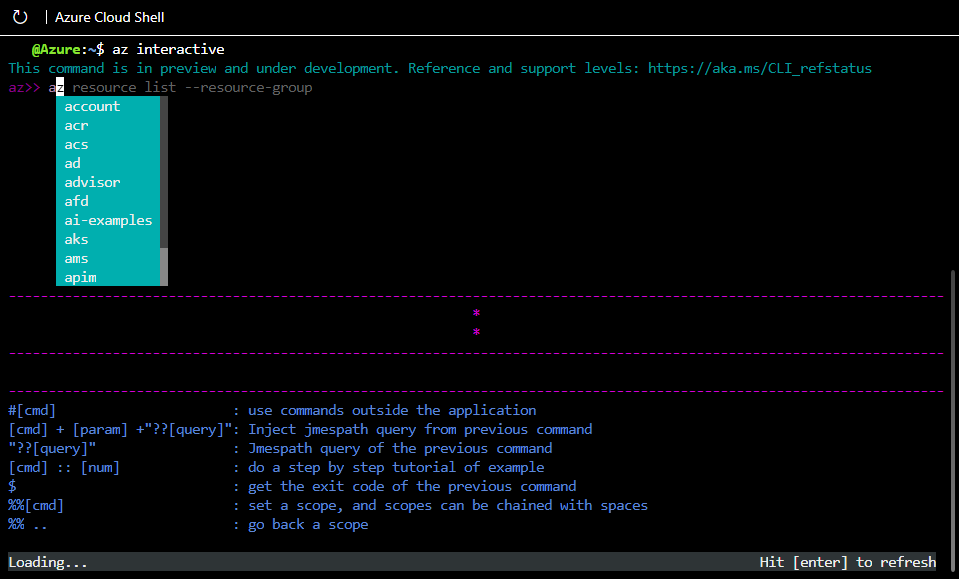
Enter az interactive to enter interactive mode.

Azure CLI

az interactive

Decide whether you wish to send telemetry data and enter YES or NO.

You may have to wait a minute or two to allow the interactive mode to fully initialize. Then, enter the letter “a” and auto-completion should start to work. If auto-completion isn’t working, erase what you’ve entered, wait a bit longer, and try again.



Once initialized, you can use the arrow keys or tab to help complete your commands. Interactive mode is set up specifically for Azure, so you don't need to enter az to start a command (but you can if you want to or are used to it). Try the upgrade or version commands again, but this time without az in front.

Azure CLI

version

Azure CLI

upgrade

The commands should have worked the same as before, and given you the same results. Use the exit command to leave interactive mode.

Azure CLI

exit

#### Task 4: Use the Azure portal

You’ll also have the option of using the Azure portal during sandbox exercises. You need to use the link provided in the exercise to access the Azure portal. Using the provided link, instead of opening the portal yourself, ensures the correct subscription is used and the exercise remains free for you to complete.

Sign in to the [Azure portal](https://portal.azure.com/learn.docs.microsoft.com) to check out the Azure web interface. Once in the portal, you can see all the services Azure has to offer as well as look around at resource groups and so on.

#### Continue

You're all set for now. We'll come back to this sandbox later in this module and actually create an Azure resource!

### Describe Azure physical infrastructure

Throughout your journey with Microsoft Azure, you’ll hear and use terms like Regions, Availability Zones, Resources, Subscriptions, and more. This module focuses on the core architectural components of Azure. The core architectural components of Azure may be broken down into two main groupings: the physical infrastructure, and the management infrastructure.

#### Physical infrastructure

The physical infrastructure for Azure starts with datacenters. Conceptually, the datacenters are the same as large corporate datacenters. They’re facilities with resources arranged in racks, with dedicated power, cooling, and networking infrastructure.

As a global cloud provider, Azure has datacenters around the world. However, these individual datacenters aren’t directly accessible. Datacenters are grouped into Azure Regions or Azure Availability Zones that are designed to help you achieve resiliency and reliability for your business-critical workloads.

The [Global infrastructure](https://infrastructuremap.microsoft.com/) site gives you a chance to interactively explore the underlying Azure infrastructure.

##### Regions

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

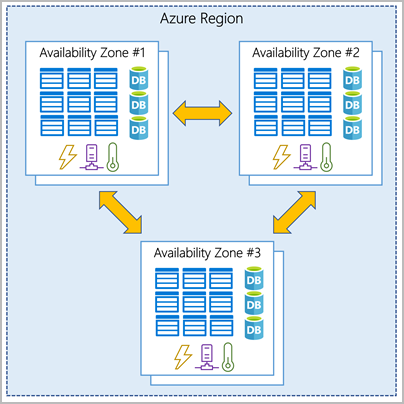
When you deploy a resource in Azure, you'll often need to choose the region where you want your resource deployed.

Note

Some services or virtual machine (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 Microsoft Entra ID, Azure Traffic Manager, and Azure DNS.

##### Availability Zones

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.



Important

To ensure resiliency, a minimum of three separate availability zones are present in all availability zone-enabled regions. However, not all Azure Regions currently support availability zones.

###### Use availability zones in your apps

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.

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

Availability zones are primarily for VMs, managed disks, load balancers, and SQL databases. Azure services that support availability zones fall into three 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).
* Non-regional services: Services are always available from Azure geographies and are resilient to zone-wide outages as well as region-wide outages.

Even with the additional resiliency that availability zones provide, it’s possible that an event could be so large that it impacts multiple availability zones in a single region. To provide even further resilience, Azure has Region Pairs.

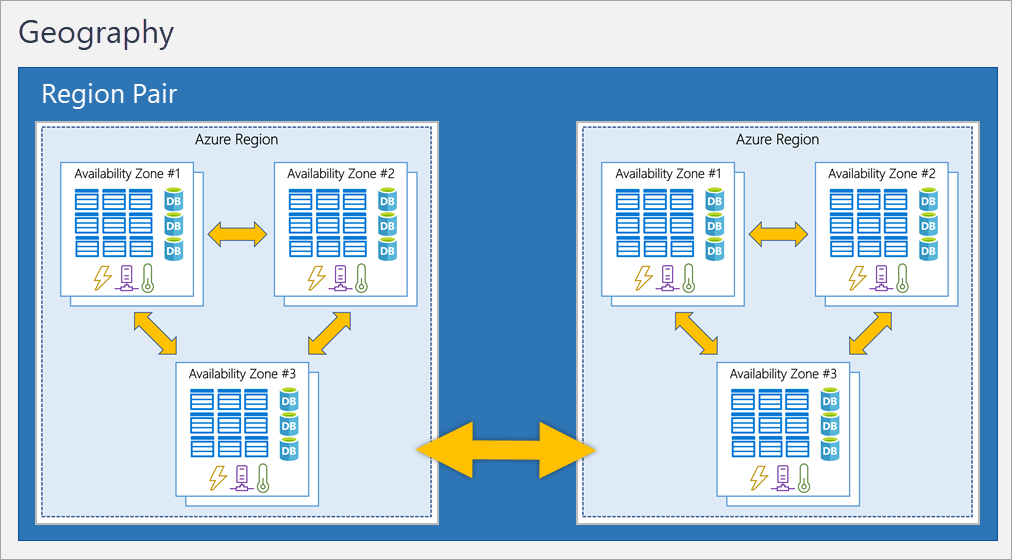
##### Region pairs

Most Azure regions are 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 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 an entire region. For example, if a region in a pair was affected by a natural disaster, services would automatically fail over to the other region in its region pair.

Important

Not all Azure services automatically replicate data or automatically fall back from a failed region to cross-replicate to another enabled region. In these scenarios, recovery and replication must be configured by the customer.

Examples of region pairs in Azure are West US paired with East US and South-East Asia paired with East Asia. Because the pair of regions are directly connected and far enough apart to be isolated from regional disasters, you can use them to provide reliable services and data redundancy.



###### Additional advantages of region pairs:

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

Important

Most regions are paired in two directions, meaning they are the backup for the region that provides a backup for them (West US and East US back each other up). However, some regions, such as West India and Brazil South, are paired in only one direction. In a one-direction pairing, the Primary region does not provide backup for its secondary region. So, even though West India’s secondary region is South India, South India does not rely on West India. West India's secondary region is South India, but South India's secondary region is Central India. Brazil South is unique because it's paired with a region outside of its geography. Brazil South's secondary region is South Central US. The secondary region of South Central US isn't Brazil South.

##### Sovereign Regions

In addition to regular regions, Azure also has sovereign regions. Sovereign regions are instances of Azure that are isolated from the main instance of Azure. You may need to use a sovereign region for compliance or legal purposes.

Azure sovereign regions include:

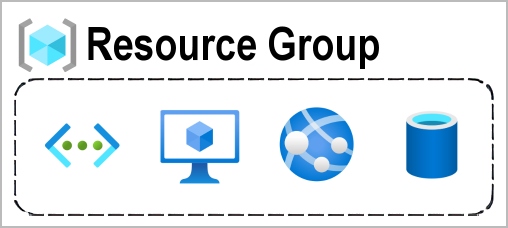
* US DoD Central, US Gov Virginia, US Gov Iowa and more: These regions are physical and logical network-isolated instances of Azure for U.S. government agencies and partners. These datacenters are operated by screened U.S. personnel and include additional compliance certifications.
* China East, China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

### Describe Azure management infrastructure

The management infrastructure includes Azure resources and resource groups, subscriptions, and accounts. Understanding the hierarchical organization will help you plan your projects and products within Azure.

#### Azure resources and resource groups

A resource is the basic building block of Azure. Anything you create, provision, deploy, etc. is a resource. Virtual Machines (VMs), virtual networks, databases, cognitive services, etc. are all considered resources within Azure.



Resource groups are simply groupings of resources. When you create a resource, you’re required to place it into a resource group. While a resource group can contain many resources, a single resource can only be in one resource group at a time. Some resources may be moved between resource groups, but when you move a resource to a new group, it will no longer be associated with the former group. Additionally, resource groups can't be nested, meaning you can’t put resource group B inside of resource group A.

Resource groups provide a convenient way to group resources together. When you apply an action to a resource group, that action will apply to all the resources within the resource group. If you delete a resource group, all the resources will be deleted. If you grant or deny access to a resource group, you’ve granted or denied access to all the resources within the resource group.

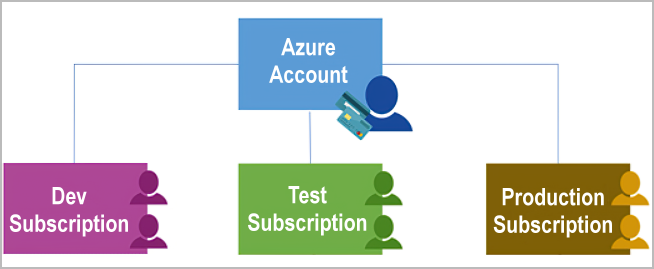
When you’re provisioning resources, it’s good to think about the resource group structure that best suits your needs.

For example, if you’re setting up a temporary dev environment, grouping all the resources together means you can deprovision all of the associated resources at once by deleting the resource group. If you’re provisioning compute resources that will need three different access schemas, it may be best to group resources based on the access schema, and then assign access at the resource group level.

There aren’t hard rules about how you use resource groups, so consider how to set up your resource groups to maximize their usefulness for you.

#### Azure subscriptions

In Azure, subscriptions are a unit of management, billing, and scale. Similar to how resource groups are a way to logically organize resources, subscriptions allow you to logically organize your resource groups and facilitate billing.



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 links to an Azure account, which is an identity in Microsoft Entra ID or in a directory that Microsoft Entra ID trusts.

An account can have multiple subscriptions, but it’s only required to have one. In a multi-subscription account, you can use the subscriptions to configure different billing models and apply different access-management policies. You can use Azure subscriptions to define boundaries around Azure products, services, and resources. There are two types of subscription boundaries that you can use:

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

##### Create additional Azure subscriptions

Similar to using resource groups to separate resources by function or access, you might want to create additional subscriptions for resource or billing management purposes. For example, you might choose to create additional subscriptions to separate:

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

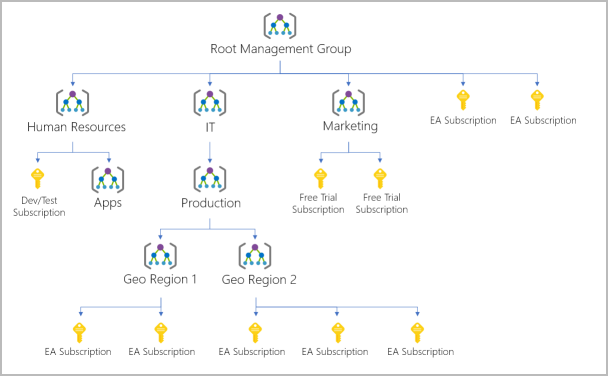
#### Azure management groups

The final piece is the management group. Resources are gathered into resource groups, and resource groups are gathered into subscriptions. If you’re just starting in Azure that might seem like enough hierarchy to keep things organized. But imagine if you’re dealing with multiple applications, multiple development teams, in multiple geographies.

If you have 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 governance conditions to the management groups. All subscriptions within a management group automatically inherit the conditions applied to the management group, the same way that resource groups inherit settings from subscriptions and resources inherit from resource groups. Management groups give you enterprise-grade management at a large scale, no matter what type of subscriptions you might have. Management groups can be nested.

#### Management group, subscriptions, and resource group hierarchy

You can build a flexible structure of management groups and subscriptions to organize your resources into a hierarchy for unified policy and access management. The following diagram shows an example of creating a hierarchy for governance by using management groups.



Some examples of how you could use management groups might be:

* **Create a hierarchy that applies a policy**. You could limit VM locations to the US West Region in a group called Production. This policy will inherit onto all the subscriptions that are descendants of that management group and will apply to all VMs under those subscriptions. This security policy can't be altered by the resource or subscription owner, which allows for improved governance.
* **Provide user access to multiple subscriptions**. By moving multiple subscriptions under a management group, you can create one Azure role-based access control (Azure RBAC) assignment on the management group. Assigning Azure RBAC at the management group level means that all sub-management groups, subscriptions, resource groups, and resources underneath that management group would also inherit those permissions. One assignment on the management group can enable users to have access to everything they need instead of scripting Azure RBAC over different subscriptions.

Important facts about management groups:

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

### Exercise - Create an Azure resource

In this exercise, you’ll use the Azure portal to create a resource. The focus of the exercise is observing how Azure resource groups populate with created resources.

Important

The sandbox should already be activated, but if the sandbox closed, reactivate the sandbox before continuing.

#### Task 1: Create a virtual machine

In this task, you’ll create a virtual machine using the Azure portal.

1. Sign in to the [Azure portal](https://portal.azure.com/learn.docs.microsoft.com).
2. Select Create a resource > Virtual Machine > Create.
3. The Create a virtual machine pane opens to the basics tab.
4. Verify or enter the following values for each setting. If a setting isn’t specified, leave the default value.

**Basics tab**

Expand table

| **Setting** | **Value** |
| --- | --- |
| Subscription | Concierge Subscription |
| Resource group | Select the resource group name that begins with **learn**. |
| Virtual machine name | my-VM |
| Region | Leave default |
| Availability options | Leave default |
| Security type | Leave default |
| Image | Leave default |
| VM architecture | Leave default |
| Run with Azure Spot discount | Unchecked |
| Size | Leave default |
| Authentication type | Password |
| Username | azureuser |
| Password | Enter a custom password |
| Confirm password | Reenter the custom password |
| Public inbound ports | None |

1. Select Review and Create.

**Important**

Product details will include a cost associated with creating the virtual machine. This is a system function. If you’re creating the VM in the Learn sandbox, you won’t actually incur any costs.

1. Select Create

Wait while the VM is provisioned. Deployment is in progress will change to Deployment is complete when the VM is ready.

#### Task 2: Verify resources created

Once the deployment is created, you can verify that Azure created not only a VM, but all of the associated resources the VM needs.

1. Select Home.
2. Select Resource groups.
3. Select the [sandbox resource group name] resource group.

You should see a list of resources in the resource group. The storage account and virtual network are associated with the Learn sandbox. However, the rest of the resources were created when you created the virtual machine. By default, Azure gave them all a similar name to help with association and grouped them in the same resource group.

Congratulations! You've created a resource in Azure and had a chance to see how resources get grouped on creation.

#### Clean up

The sandbox automatically cleans up your resources when you're finished with this module.

When you're working in your own subscription, it's a good idea at the end of a project to identify whether you still need the resources you created. Resources that you leave running can cost you money. You can delete resources individually or delete the resource group to delete the entire set of resources.

### [Knowledge check](https://learn.microsoft.com/en-us/training/modules/describe-core-architectural-components-of-azure/8-knowledge-check)

### Summary

In this module, you learned about the physical and management structure of Microsoft Azure. You were introduced to the relationship between datacenters, availability zones, and regions. You explored how the infrastructure supports the benefits of the cloud, such as high availability and reliability. You also learned about the management infrastructure of Azure. You explored how resources and resource groups are related, and how subscriptions and management groups can help manage resources.

#### Learning objectives

You should now be able to:

* Describe Azure regions, region pairs, and sovereign regions.
* Describe Availability Zones.
* Describe Azure datacenters.
* Describe Azure resources and Resource Groups.
* Describe subscriptions.
* Describe management groups.
* Describe the hierarchy of resource groups, subscriptions, and management groups.

## Describe Azure compute and networking services

### Introduction

This module introduces you to the compute and networking services of Azure. You learn about three of the compute options (virtual machines, containers, and Azure functions). You also learn about some of the networking features, such as Azure virtual networks, Azure DNS, and Azure ExpressRoute.

#### Learning objectives

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

* Compare compute types, including container instances, virtual machines, and functions.
* Describe virtual machine options, including virtual machines (VMs), virtual machine scale sets, virtual machine availability sets, and Azure Virtual Desktop.
* Describe resources required for virtual machines.
* Describe application hosting options, including Azure Web Apps, containers, and virtual machines.
* Describe virtual networking, including the purpose of Azure Virtual Networks, Azure virtual subnets, peering, Azure DNS, VPN Gateway, and ExpressRoute.
* Define public and private endpoints.

### Describe Azure virtual machines

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

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

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

You can even create or use an already created image to rapidly provision VMs. You can create and provision a VM in minutes when you select a preconfigured VM image. An image is a template used to create a VM and may already include an OS and other software, like development tools or web hosting environments.

#### Scale VMs in Azure

You can run single VMs for testing, development, or minor tasks. Or you can group VMs together to provide high availability, scalability, and redundancy. Azure can also manage the grouping of VMs for you with features such as scale sets and availability sets.

##### Virtual machine scale sets

Virtual machine scale sets let you create and manage a group of identical, load-balanced VMs. If you simply created multiple VMs with the same purpose, you’d need to ensure they were all configured identically and then set up network routing parameters to ensure efficiency. You’d also have to monitor the utilization to determine if you need to increase or decrease the number of VMs.

Instead, with virtual machine scale sets, Azure automates most of that work. Scale sets allow you to centrally manage, configure, and update a large number of VMs in minutes. The number of VM instances can automatically increase or decrease in response to demand, or you can set it to scale based on a defined schedule. Virtual machine scale sets also automatically deploy a load balancer to make sure that your resources are being used efficiently. With virtual machine scale sets, you can build large-scale services for areas such as compute, big data, and container workloads.

##### Virtual machine availability sets

Virtual machine availability sets are another tool to help you build a more resilient, highly available environment. Availability sets are designed to ensure that VMs stagger updates and have varied power and network connectivity, preventing you from losing all your VMs with a single network or power failure.

Availability accomplish these objectives by grouping VMs in two ways: update domain and fault domain.

* **Update domain**: The update domain groups VMs that can be rebooted at the same time. This setup allows you to apply updates while knowing that only one update domain grouping is offline at a time. All of the machines in one update domain update. An update group going through the update process is given a 30-minute time to recover before maintenance on the next update domain starts.
* **Fault domain**: The fault domain groups your VMs by common power source and network switch. By default, an availability set splits your VMs across up to three fault domains. This helps protect against a physical power or networking failure by having VMs in different fault domains (thus being connected to different power and networking resources).

Best of all, there’s no additional cost for configuring an availability set. You only pay for the VM instances you create.

#### Examples of when to use VMs

Some common examples or use cases for virtual machines include:

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

#### Move to the cloud with VMs

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

#### VM Resources

When you provision a VM, you’ll also have the chance to pick the resources that are associated with that VM, including:

* Size (purpose, number of processor cores, and amount of RAM)
* Storage disks (hard disk drives, solid state drives, etc.)
* Networking (virtual network, public IP address, and port configuration)

### Exercise - Create an Azure virtual machine

In this exercise, you create an Azure virtual machine (VM) and install Nginx, a popular web server.

You could use the Azure portal, the Azure CLI, Azure PowerShell, or an Azure Resource Manager (ARM) template.

In this instance, you're going to use the Azure CLI.

#### Task 1: Create a Linux virtual machine and install Nginx

Use the following Azure CLI commands to create a Linux VM and install Nginx. After your VM is created, you'll use the Custom Script Extension to install Nginx. The Custom Script Extension is an easy way to download and run scripts on your Azure VMs. It's just one of the many ways you can configure the system after your VM is up and running.

1. From Cloud Shell, run the following az vm create command to create a Linux VM:

Azure CLI

az vm create \

--resource-group "[sandbox resource group name]" \

--name my-vm \

--public-ip-sku Standard \

--image Ubuntu2204 \

--admin-username azureuser \

--generate-ssh-keys

Your VM takes a few moments to come up. You named the VM **my-vm**. You use this name to refer to the VM in later steps.

1. Run the following az vm extension set command to configure Nginx on your VM:

Azure CLI

az vm extension set \

--resource-group "[sandbox resource group name]" \

--vm-name my-vm \

--name customScript \

--publisher Microsoft.Azure.Extensions \

--version 2.1 \

--settings '{"fileUris":["https://raw.githubusercontent.com/MicrosoftDocs/mslearn-welcome-to-azure/master/configure-nginx.sh"]}' \

--protected-settings '{"commandToExecute": "./configure-nginx.sh"}'

This command uses the Custom Script Extension to run a Bash script on your VM. The script is stored on GitHub. While the command runs, you can choose to [examine the Bash script](https://raw.githubusercontent.com/MicrosoftDocs/mslearn-welcome-to-azure/master/configure-nginx.sh) from a separate browser tab. To summarize, the script:

* 1. Runs apt-get update to download the latest package information from the internet. This step helps ensure that the next command can locate the latest version of the Nginx package.
  2. Installs Nginx.
  3. Sets the home page, */var/www/html/index.html*, to print a welcome message that includes your VM's host name.

Continue

This exercise is complete for now. The sandbox keeps running, and you come back to this point in a few units to update the network configuration so you can get to the website.

### Describe Azure virtual desktop

Another type of virtual machine is the Azure Virtual Desktop. Azure Virtual Desktop is a desktop and application virtualization service that runs on the cloud. It enables you to use a cloud-hosted version of Windows from any location. Azure Virtual Desktop works across devices and operating systems, and works with apps that you can use to access remote desktops or most modern browsers.

The following video gives you an overview of Azure Virtual Desktop:

[Video](https://learn.microsoft.com/en-us/training/modules/describe-azure-compute-networking-services/4-virtual-desktop)

#### Enhance security

Azure Virtual Desktop provides centralized security management for users' desktops with Microsoft Entra ID. You can enable multifactor authentication to secure user sign-ins. You can also secure access to data by assigning granular role-based access controls (RBACs) to users.

With Azure Virtual Desktop, the data and apps are separated from the local hardware. The actual desktop and apps are running in the cloud, meaning the risk of confidential data being left on a personal device is reduced. Additionally, user sessions are isolated in both single and multi-session environments.

#### Multi-session Windows 10 or Windows 11 deployment

Azure Virtual Desktop lets you use Windows 10 or Windows 11 Enterprise multi-session, the only Windows client-based operating system that enables multiple concurrent users on a single VM. Azure Virtual Desktop also provides a more consistent experience with broader application support compared to Windows Server-based operating systems.

### Describe Azure containers

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. Containers are lightweight and designed to be created, scaled out, and stopped dynamically. It's possible to create and deploy virtual machines as application demand increases, but containers are a lighter weight, more agile method. Containers are designed to allow you to respond to changes on demand. With containers, you can quickly restart if there's a crash or hardware interruption. One of the most popular container engines is Docker, and Azure supports Docker.

#### Compare virtual machines to containers

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

[Video](https://learn.microsoft.com/en-us/training/modules/describe-azure-compute-networking-services/5-containers)

#### Azure Container Instances

Azure Container Instances offer the fastest and simplest way to run a container in Azure; without having to manage any virtual machines or adopt any additional services. Azure Container Instances are a platform as a service (PaaS) offering. Azure Container Instances allow you to upload your containers and then the service runs the containers for you.

#### Azure Container Apps

Azure Container Apps are similar in many ways to a container instance. They allow you to get up and running right away, they remove the container management piece, and they're a PaaS offering. Container Apps have extra benefits such as the ability to incorporate load balancing and scaling. These other functions allow you to be more elastic in your design.

#### Azure Kubernetes Service

Azure Kubernetes Service (AKS) is a container orchestration service. An orchestration service manages the lifecycle of containers. When you're deploying a fleet of containers, AKS can make fleet management simpler and more efficient.

#### Use containers in your solutions

Containers are often used to create solutions by using a microservice architecture. This architecture is where you break solutions into smaller, independent pieces. For example, you might split a website into a container hosting your front end, another hosting your back end, and a third for storage. This split allows you to separate portions of your app into logical sections that can be maintained, scaled, or updated independently.

Imagine your website back-end reaches capacity, but the front end and storage aren't stressed. With containers, you could scale the back-end separately to improve performance. If something necessitated such a change, you could also choose to change the storage service or modify the front end without impacting any of the other components.

### Describe Azure functions

Azure Functions is an event-driven, serverless compute option that doesn’t require maintaining virtual machines or containers. If you build an app using VMs or containers, those resources have to be “running” in order for your app to function. With Azure Functions, an event wakes the function, alleviating the need to keep resources provisioned when there are no events.

#### Serverless computing in Azure

[**Video**](https://learn.microsoft.com/en-us/training/modules/describe-azure-compute-networking-services/6-functions)

#### Benefits of Azure Functions

Using Azure Functions is ideal when you're only concerned about the code running your service and not about the underlying platform or infrastructure. 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 may be a good choice when demand is variable.

Azure Functions runs your code when it triggers and automatically deallocates resources when the function is finished. In this model, Azure only charges you for the CPU time used while your function runs.

Functions can be either stateless or stateful. When they're stateless (the default), they behave as if they restart every time they respond to an event. Every time the function runs, it **starts fresh** and does not remember anything from the previous run. When they're stateful (called Durable Functions), a context is passed through the function to track prior activity. These remember past actions, so they can track and continue previous work.

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

### Describe application hosting options

If you need to host your application on Azure, you might initially turn to a virtual machine (VM) or containers. Both VMs and containers provide excellent hosting solutions. VMs give you maximum control of the hosting environment and allow you to configure it exactly how you want. VMs also may be the most familiar hosting method if you’re new to the cloud. Containers, with the ability to isolate and individually manage different aspects of the hosting solution, can also be a robust and compelling option.

There are other hosting options that you can use with Azure, including Azure App Service.

#### Azure App Service

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

Azure App Service is a robust hosting option that you can use to host your apps in Azure. Azure App Service lets you focus on building and maintaining your app, and Azure focuses on keeping the environment up and running.

Azure App Service is an HTTP-based service for hosting web applications, REST APIs, and mobile back ends. It supports multiple languages, including .NET, .NET Core, Java, Ruby, Node.js, PHP, or Python. It also supports both Windows and Linux environments.

#### Types of app services

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

* Web apps
* API apps
* WebJobs
* Mobile apps

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

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

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

##### Web apps

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

##### API apps

Much like hosting a website, you can build REST-based web APIs by using your choice of language and framework. You get full Swagger support and the ability to package and publish your API in Azure Marketplace. The produced apps can be consumed from any HTTP- or HTTPS-based client.

##### WebJobs

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

##### Mobile apps

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

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

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

### Describe Azure virtual networking

Azure virtual networks and virtual subnets 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 an extension of your on-premises network with resources that link other Azure resources.

Azure virtual networks provide the following key networking capabilities:

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

Azure virtual networking supports both public and private endpoints to enable communication between external or internal resources with other internal resources.

* Public endpoints have a public IP address and can be accessed from anywhere in the world.
* Private endpoints exist within a virtual network and have a private IP address from within the address space of that virtual network.

#### Isolation and segmentation

Azure virtual network allows you to create multiple isolated virtual networks. When you set up a virtual network, you define a private IP address space by using either public or private IP address ranges. The IP range only exists within the virtual network and isn't internet routable. You can divide that IP address space into subnets and allocate part of the defined address space to each named subnet.

For name resolution, you can use the name resolution service built into Azure. You also can configure the virtual network to use either an internal or an external DNS server.

#### Internet communications

You can enable incoming connections from the internet by assigning a public IP address to an Azure resource, or putting the resource behind a public load balancer.

#### Communicate between Azure resources

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

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

#### Communicate with on-premises resources

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

* Point-to-site virtual private network connections are from a computer outside your organization back into your corporate network. In this case, the client computer initiates an encrypted VPN connection to connect to the Azure virtual network.
* Site-to-site virtual private networks link 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 provides a dedicated private connectivity to Azure that doesn't travel over the internet. ExpressRoute is useful for environments where you need greater bandwidth and even higher levels of security.

#### 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 allow 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 (BGP) works with Azure VPN gateways, Azure Route Server, or Azure 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 are Azure resources 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 are specialized VMs that can be compared to a hardened network appliance. A network virtual appliance carries out a particular network function, such as running a firewall or performing wide area network (WAN) optimization.

#### Connect virtual networks

You can link virtual networks together by using virtual network peering. Peering allows two virtual networks to connect directly to each other. Network traffic between peered networks is private, and travels on the Microsoft backbone network, never entering the public internet. Peering enables resources in each virtual network to communicate with each other. These virtual networks can be in separate regions. This feature allows you to create a global interconnected network through Azure.

User-defined routes (UDR) allow you to control the routing tables between subnets within a virtual network or between virtual networks. This allows for greater control over network traffic flow.

### Exercise - Configure network access

In this exercise, you configure the access to the virtual machine (VM) you created earlier in this module.

Important

The Microsoft Learn sandbox should still be running. If the sandbox timed out, you'll need to redo the previous exercise (**Exercise - Create an Azure virtual machine**).

To verify the VM you created previously is still running, use the following command:

Azure CLI

az vm list

If you receive an empty response [], you need to complete the first exercise in this module again. If the result lists your current VM and its settings, you may continue.

Right now, When you create a Virtual Machine (VM) in Azure and install a web server like Nginx, the server listens for incoming HTTP requests on port 80. However, Azure blocks most inbound traffic by default for security reasons.

To make your Nginx server accessible from the internet, you need to open port 80 using a Network Security Group (NSG). This allows users to connect to your website using a web browser.

#### Task 1: Access your web server

In this procedure, you get the IP address for your VM and attempt to access your web server's home page.

1. Run the following az vm list-ip-addresses command to get your VM's IP address and store the result as a Bash variable:

Azure CLI

IPADDRESS="$(az vm list-ip-addresses \

--resource-group "[sandbox resource group name]" \

--name my-vm \

--query "[].virtualMachine.network.publicIpAddresses[\*].ipAddress" \

--output tsv)"

1. Run the following curl command to download the home page:

Bash

curl --connect-timeout 5 http://$IPADDRESS

The --connect-timeout argument specifies to allow up to five seconds for the connection to occur. After five seconds, you see an error message that states that the connection timed out:

Output

curl: (28) Connection timed out after 5001 milliseconds

This message means that the VM wasn't accessible within the timeout period.

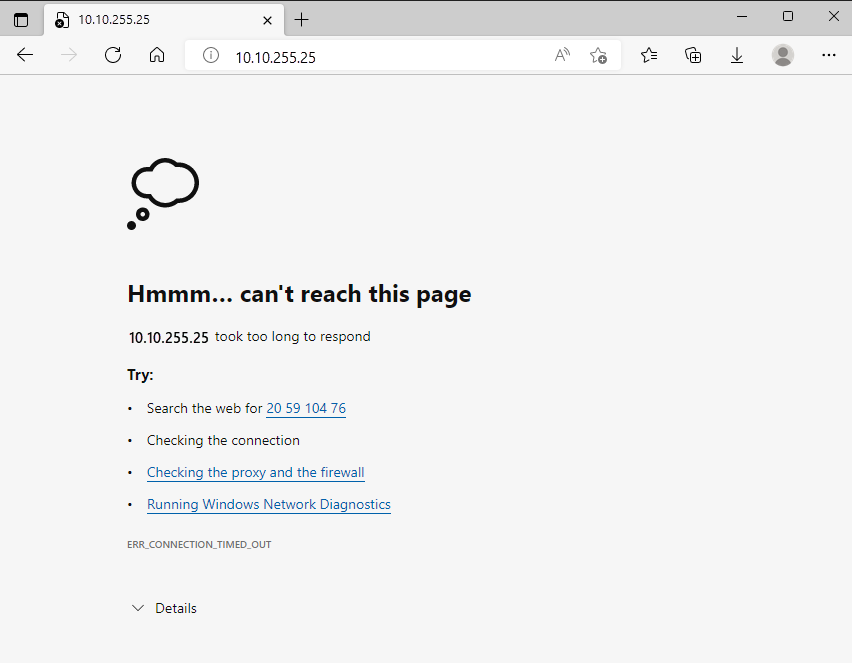
1. As an optional step, try to access the web server from a browser:
   1. Run the following to print your VM's IP address to the console:

Bash

echo $IPADDRESS

You see an IP address, for example, *23.102.42.235*.

* 1. Copy the IP address that you see to the clipboard.
  2. Open a new browser tab and go to your web server. After a few moments, you see that the connection isn't happening. If you wait for the browser to time out, you see something like this:



* 1. Keep this browser tab open for later.

#### Task 2: List the current network security group rules

Your web server wasn't accessible. To find out why, let's examine your current NSG rules.

1. Run the following az network nsg list command to list the network security groups that are associated with your VM:

Azure CLI

az network nsg list \

--resource-group "[sandbox resource group name]" \

--query '[].name' \

--output tsv

You see this output:

Output

my-vmNSG

Every VM on Azure is associated with at least one network security group. In this case, Azure created an NSG for you called *my-vmNSG*.

1. Run the following az network nsg rule list command to list the rules associated with the NSG named *my-vmNSG*:

Azure CLI

az network nsg rule list \

--resource-group "[sandbox resource group name]" \

--nsg-name my-vmNSG

You see a large block of text in JSON format in the output. In the next step, you'll run a similar command that makes this output easier to read.

1. Run the az network nsg rule list command a second time. This time, use the --query argument to retrieve only the name, priority, affected ports, and access (**Allow** or **Deny**) for each rule. The --output argument formats the output as a table so that it's easy to read.

Azure CLI

az network nsg rule list \

--resource-group "[sandbox resource group name]" \

--nsg-name my-vmNSG \

--query '[].{Name:name, Priority:priority, Port:destinationPortRange, Access:access}' \

--output table

You see this output:

Output

Name Priority Port Access

----------------- ---------- ------ --------

default-allow-ssh 1000 22 Allow

You see the default rule, *default-allow-ssh*. This rule allows inbound connections over port 22 (SSH). SSH (Secure Shell) is a protocol that's used on Linux to allow administrators to access the system remotely. The priority of this rule is 1000. Rules are processed in priority order, with lower numbers processed before higher numbers.

By default, a Linux VM's NSG allows network access only on port 22. This port enables administrators to access the system. You need to also allow inbound connections on port 80, which allows access over HTTP.

#### Task 3: Create the network security rule

Here, you create a network security rule that allows inbound access on port 80 (HTTP).

1. Run the following az network nsg rule create command to create a rule called *allow-http* that allows inbound access on port 80:

Azure CLI

az network nsg rule create \

--resource-group "[sandbox resource group name]" \

--nsg-name my-vmNSG \

--name allow-http \

--protocol tcp \

--priority 100 \

--destination-port-range 80 \

--access Allow

For learning purposes, here you set the priority to 100. In this case, the priority doesn't matter. You would need to consider the priority if you had overlapping port ranges.

1. To verify the configuration, run az network nsg rule list to see the updated list of rules:

Azure CLI

az network nsg rule list \

--resource-group "[sandbox resource group name]" \

--nsg-name my-vmNSG \

--query '[].{Name:name, Priority:priority, Port:destinationPortRange, Access:access}' \

--output table

You see both the *default-allow-ssh* rule and your new rule, *allow-http*:

Output

Name Priority Port Access

----------------- ---------- ------ --------

default-allow-ssh 1000 22 Allow

allow-http 100 80 Allow

#### Task 4: Access your web server again

Now that you configured network access to port 80, let's try to access the web server a second time.

 Note

After you update the NSG, it may take a few moments before the updated rules propagate. Retry the next step, with pauses between attempts, until you get the desired results.

1. Run the same curl command that you ran earlier:

Bash

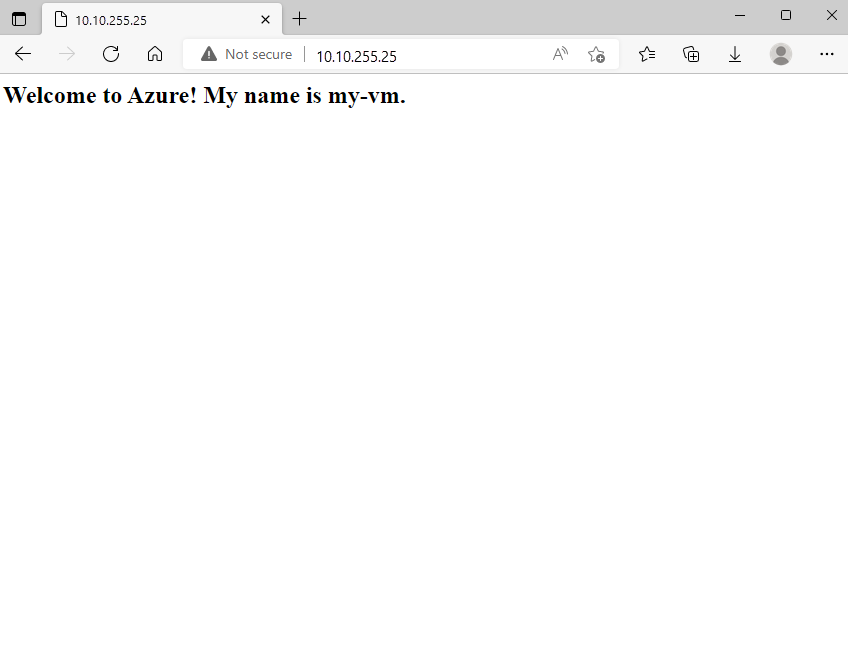
curl --connect-timeout 5 http://$IPADDRESS

You see this response:

HTML

<html><body><h2>Welcome to Azure! My name is my-vm.</h2></body></html>

1. As an optional step, refresh your browser tab that points to your web server. You see the home page:



Nice work. In practice, you can create a standalone network security group that includes the inbound and outbound network access rules you need. If you have multiple VMs that serve the same purpose, you can assign that NSG to each VM at the time you create it. This technique enables you to control network access to multiple VMs under a single, central set of rules.

#### Clean up

The sandbox automatically cleans up your resources when you're finished with this module.

When you're working in your own subscription, it's a good idea at the end of a project to identify whether you still need the resources you created. Resources that you leave running can cost you money. You can delete resources individually or delete the resource group to delete the entire set of resources.

### Describe Azure virtual private networks

A virtual private network (VPN) uses an encrypted tunnel within another network. VPNs are 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. VPNs can enable networks to safely and securely share sensitive information.

#### VPN gateways

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

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

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

When setting up a VPN gateway, you must specify the type of VPN - either policy-based or route-based. The primary distinction between these two types is how they determine which traffic needs encryption. In Azure, regardless of the VPN type, the method of authentication employed is a preshared key.

* Policy-based VPN gateways specify statically the IP address of packets that should be encrypted through each tunnel. This type of device evaluates every data packet against those sets of IP addresses to choose the tunnel where that packet is going to be sent through.
* In Route-based gateways, IPSec tunnels are modeled as a network interface or virtual tunnel interface. IP routing (either static routes or dynamic routing protocols) decides which one of these tunnel interfaces to use when sending each packet. Route-based VPNs are the preferred connection method for on-premises devices. They're more resilient to topology changes such as the creation of new subnets.

Use a route-based VPN gateway if you need any of the following types of connectivity:

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

#### High-availability scenarios

If you’re configuring a VPN to keep your information safe, you also want to be sure that it’s a highly available and fault tolerant VPN configuration. There are a few ways to maximize the resiliency of your VPN gateway.

#### Active/standby

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

#### Active/active

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

#### ExpressRoute failover

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

#### Zone-redundant gateways

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