

AZ-305 Microsoft Azure Architect Design Prerequisites

Describe the core architectural components of Azure

Introduction

Completed

- 1 minute

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.

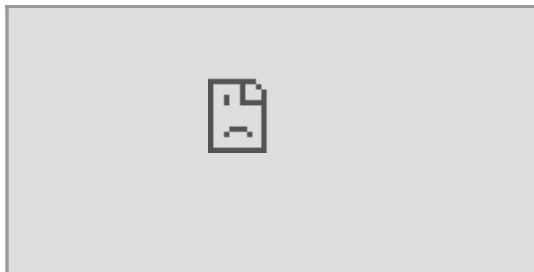
[Continue](#)

Need help? See our troubleshooting guide or provide specific feedback by reporting an issue .

What is Microsoft Azure

Completed

- 4 minutes



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.

What does Azure offer?

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

- **Be ready for the future** : Continuous innovation from Microsoft supports your development today and your product visions for tomorrow.
- **Build on your terms** : You have choices. With a commitment to open source, and support for all languages and frameworks, you can build how you want and deploy where you want.
- **Operate hybrid seamlessly** : On-premises, in the cloud, and at the edge, we'll meet you where you are. Integrate and manage your environments with tools and services designed for a hybrid cloud solution.
- **Trust your cloud** : Get security from the ground up, backed by a team of experts, and proactive compliance trusted by enterprises, governments, and startups.

What can I do with Azure?

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

Many teams start exploring the cloud by moving their existing applications to virtual machines (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.

[Continue](#)

Need help? See our troubleshooting guide or provide specific feedback by reporting an issue .

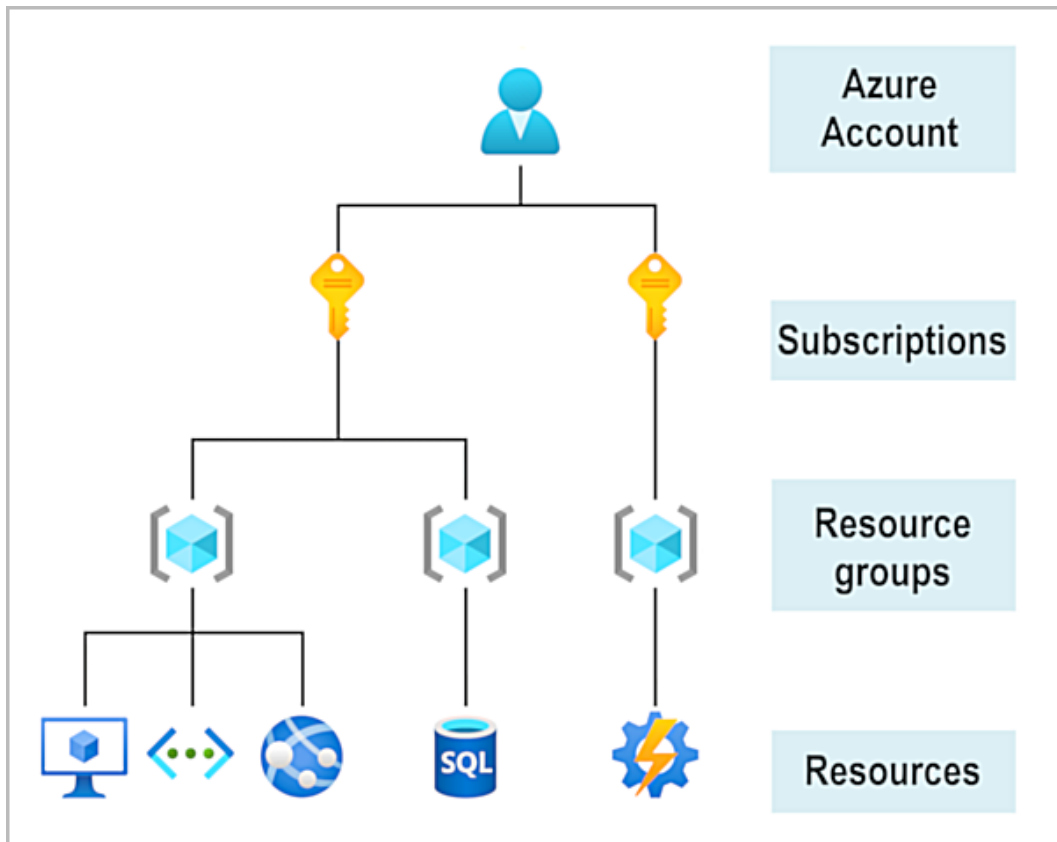
[Get started with Azure accounts](#)

Completed

- 4 minutes

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

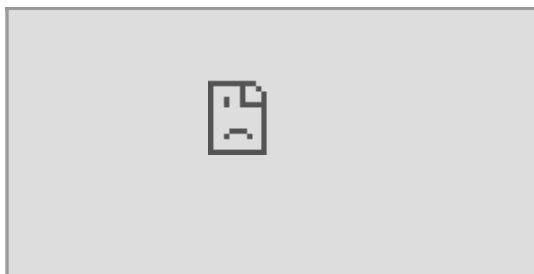
subscriptions for development, marketing, and sales departments. After you've created an Azure subscription, you can start creating Azure resources within each subscription.



If you're new to Azure, you can sign up for a free account on the Azure website to start exploring at no cost to you. When you're ready, you can choose to upgrade your free account. You can 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.



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](#) 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](#) 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.

[Continue](#)

Need help? See our troubleshooting guide or provide specific feedback by reporting an issue .

[Exercise - Explore the Learn sandbox](#)

Completed

- 10 minutes

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.

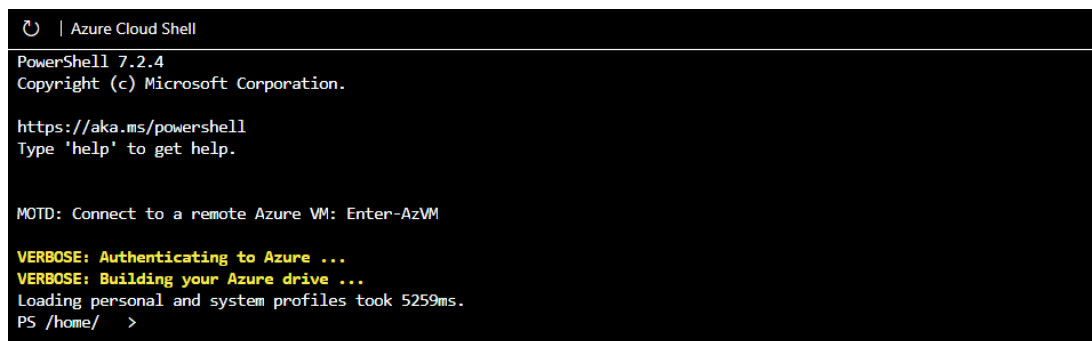
Activate the Learn Sandbox

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.

A screenshot of the Azure Cloud Shell interface. The title bar at the top says "Azure Cloud Shell". Below it, the PowerShell version "PowerShell 7.2.4" and copyright "Copyright (c) Microsoft Corporation." are displayed. The prompt "https://aka.ms/powershell" and "Type 'help' to get help." are shown. A message "MOTD: Connect to a remote Azure VM: Enter-AzVM" is visible. Below that, two yellow status messages are shown: "VERBOSE: Authenticating to Azure ..." and "VERBOSE: Building your Azure drive ...". A line of text indicates "Loading personal and system profiles took 5259ms." The prompt "PS /home/ >" is at the bottom.

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.

```
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.

```
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.

```
bash
```

```
Azure Cloud Shell
PS /home/ ~ > bash
@Azure:~$
```

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.

Get-date

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

```
Azure Cloud Shell
PS /home/ ~ > bash
@Azure:~$ Get-date
bash: Get-date: command not found
@Azure:~$
```

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

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.

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.

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.

```
Azure Cloud Shell

@Azure:~$ az interactive
This command is in preview and under development. Reference and support levels: https://aka.ms/CLI_refstatus
az>> az resource list --resource-group
account
acr
acs
ad
advisor
afd
ai-examples
aks
ams
apim

-----
*
*
-----

# [cmd] : use commands outside the application
[cmd] + [param] + "??[query]": Inject jmespath query from previous command
"??[query]" : Jmespath query of the previous command
[cmd] :: [num] : do a step by step tutorial of example
$ : get the exit code of the previous command
%%[cmd] : set a scope, and scopes can be chained with spaces
%% .. : go back a scope

Loading... Hit [enter] to refresh
```

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.

```
version
upgrade
```

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

```
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](#) 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!

[Continue](#)

Need help? See our troubleshooting guide or provide specific feedback by reporting an issue .

Describe Azure physical infrastructure

Completed

- 6 minutes

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](#) 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.

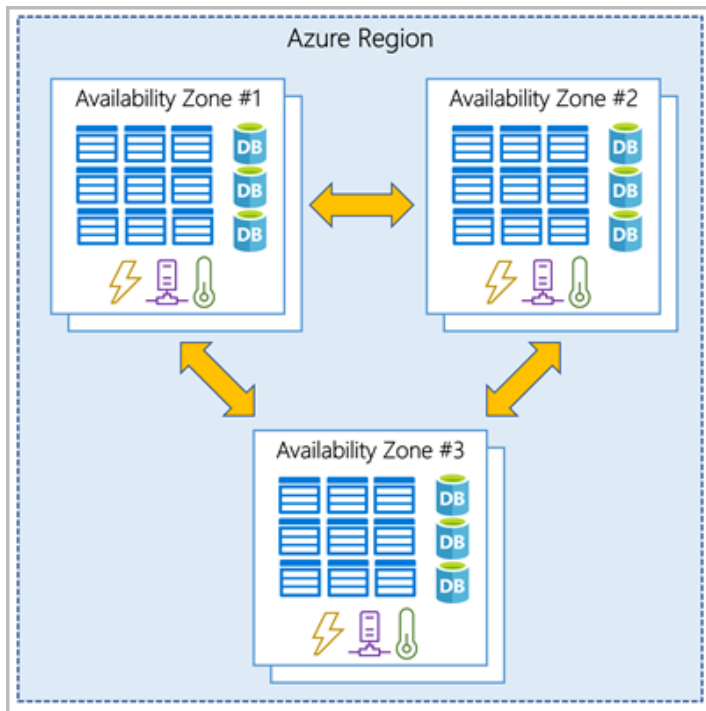
Note

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.

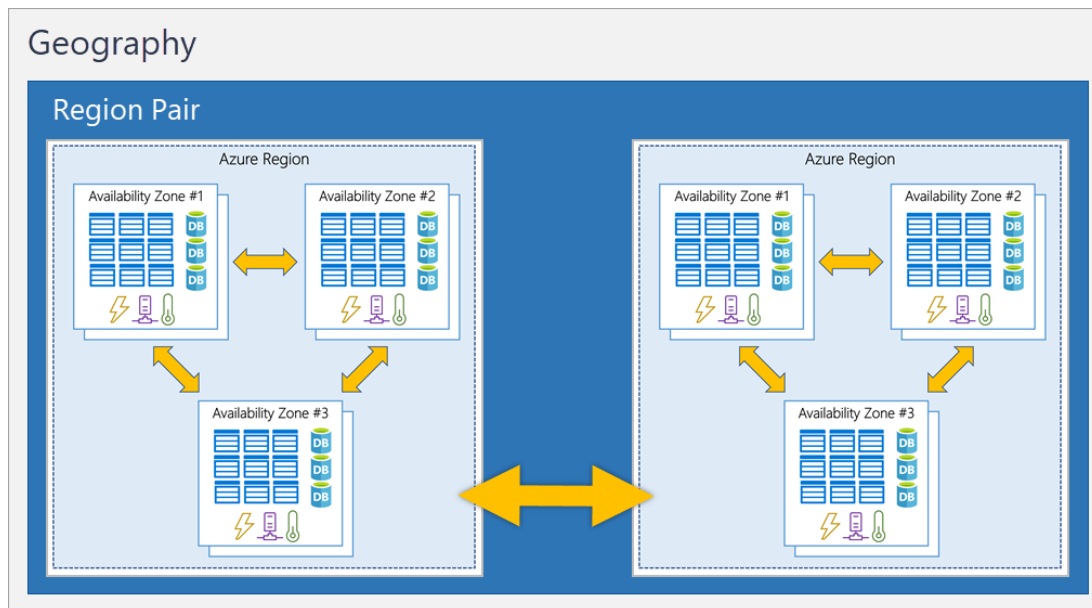
Region pairs

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.

[Continue](#)

Need help? See our troubleshooting guide or provide specific feedback by reporting an issue .

[Describe Azure management infrastructure](#)

Completed

- 7 minutes

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.

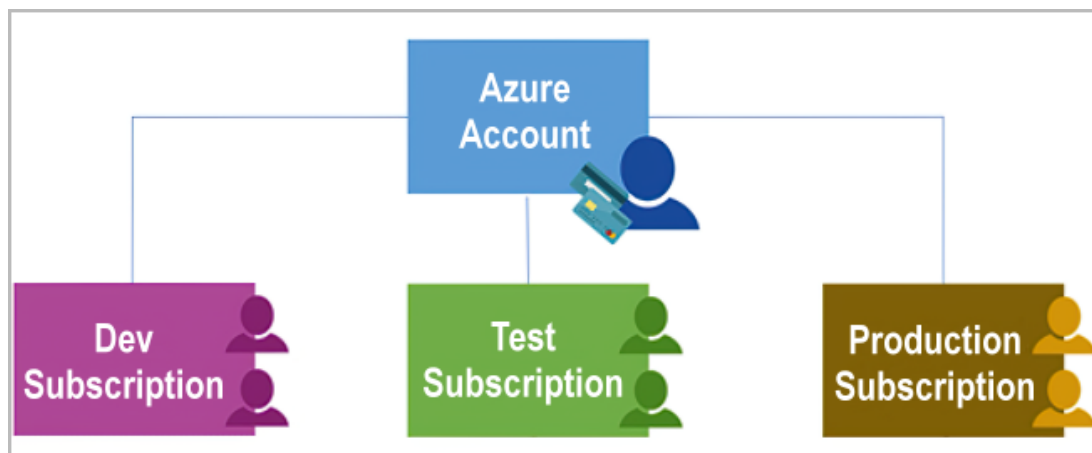
When you're provisioning resources, it's good to think about the resource group structure that best suits your needs.

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.

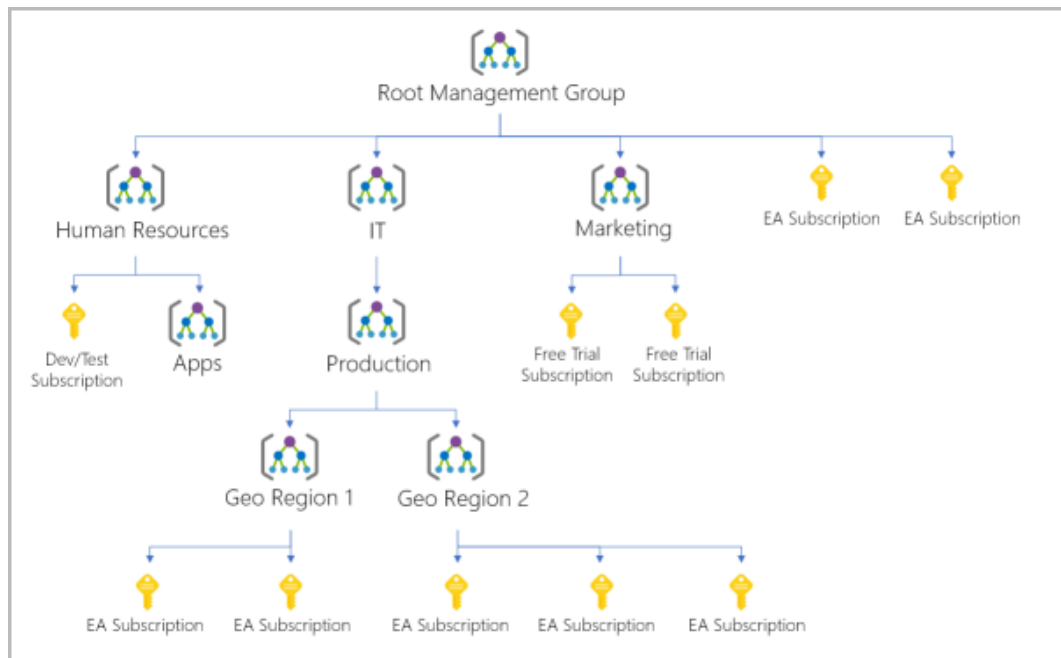
Azure management groups

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.

[Continue](#)

Need help? See our troubleshooting guide or provide specific feedback by reporting an issue .

Exercise - Create an Azure resource

Completed

- 10 minutes

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](#).
2. Select Create a resource > Compute > 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

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

5. 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.

6. 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.

[Continue](#)

Need help? See our troubleshooting guide or provide specific feedback by reporting an issue .

Knowledge check

Completed

- 4 minutes

Choose the best response for each question. Then select **Check your answers** .

Check your knowledge

1.

How many resource groups can a resource be in at the same time?

☐

One

☐

Two

☐

Three

2.

What happens to the resources within a resource group when an action or setting at the Resource Group level is applied?

☐

Current resources inherit the setting, but future resources don't.

☐

Future resources inherit the setting, but current ones don't.

☐

The setting is applied to current and future resources.

3.

What Azure feature replicates resources across regions that are at least 300 miles away from each other?

☐

Region pairs

☐

Availability Zones

☐

Sovereign regions

Check your answers

You must answer all questions before checking your work.

[Continue](#)

Need help? See our troubleshooting guide or provide specific feedback by reporting an issue .

[Summary](#)

Completed

- 2 minutes

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.

[Continue](#)

Need help? See our troubleshooting guide or provide specific feedback by reporting an issue .

Describe Azure compute and networking services

Introduction

Completed

- 1 minute

In this module, you'll be introduced to the compute and networking services of Azure. You'll learn about three of the compute options (virtual machines, containers, and Azure functions). You'll 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.

Continue

Need help? See our troubleshooting guide or provide specific feedback by reporting an issue .

Describe Azure virtual machines

Completed

- 6 minutes

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 sets do this 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 allows you to apply updates while knowing that only one update domain grouping will be offline at a time. All of the machines in one update domain will be updated. 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 will split 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)

[Continue](#)

Need help? See our troubleshooting guide or provide specific feedback by reporting an issue .

[Exercise - Create an Azure virtual machine](#)

Completed

- 10 minutes

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:

```
az vm create \
  --resource-group <rgn>[sandbox resource group name]</rgn> \
  --name my-vm \
  --public-ip-sku Standard \
  --image Ubuntu2204 \
  --admin-username azureuser \
  --generate-ssh-keys
```

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

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

```
az vm extension set \
  --resource-group <rgn>[sandbox resource group name]</rgn> \
  --vm-name my-vm \
  --name customScript \
  --publisher Microsoft.Azure.Extensions \
  --version 2.1 \
  --settings '{"fileUris":["https://raw.githubusercontent.com/MicrosoftDocs/mslearn-welcome-to-azure/master/configure-nginx.sh"]}' \
  --protected-settings '{"commandToExecute": "./configure-nginx.sh"}'
```

This command uses the Custom Script Extension to run a Bash script on your VM. The script is stored on GitHub. While the command runs, you can choose to [examine the Bash script](#) from a separate browser tab. To summarize, the script:

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

That's all for this exercise. The sandbox will keep running, and you'll come back to this point in a few units to update the network configuration so you can get to the website.

[Continue](#)

Need help? See our troubleshooting guide or provide specific feedback by reporting an issue .

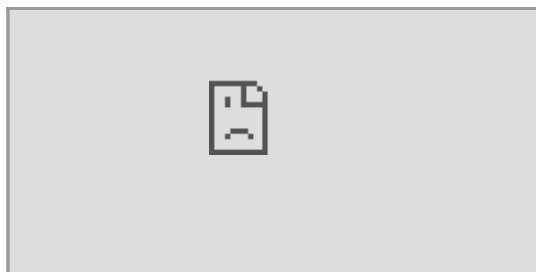
Describe Azure virtual desktop

Completed

- 5 minutes

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:



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.

[Continue](#)

Need help? See our troubleshooting guide or provide specific feedback by reporting an issue .

Describe Azure containers

Completed

- 6 minutes

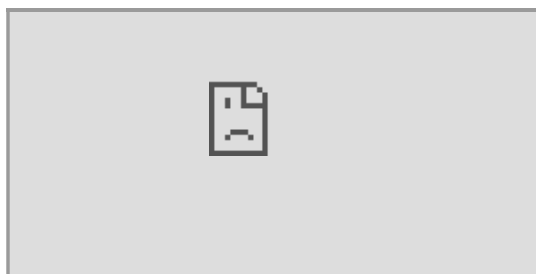
While virtual machines are an excellent way to reduce costs versus the investments that are necessary for physical hardware, they're still limited to a single operating system per virtual machine. If you want to run multiple instances of an application on a single host machine, containers are an excellent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

What are containers?

Containers are a virtualization environment. Much like running multiple virtual machines on a single physical host, you can run multiple containers on a single physical or virtual host. Unlike virtual machines, you don't manage the operating system for a container. Virtual machines appear to be an instance of an operating system that you can connect to and manage. 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:



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 will run 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 has reached capacity but the front end and storage aren't being 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.

[Continue](#)

Need help? See our troubleshooting guide or provide specific feedback by reporting an issue .

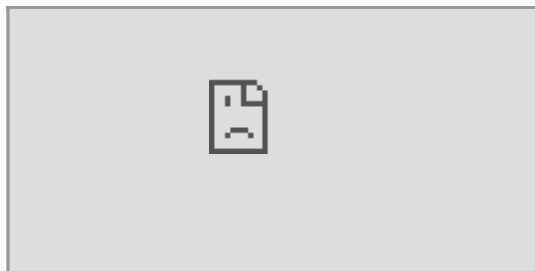
Describe Azure functions

Completed

- 4 minutes

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



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's triggered and automatically deallocates resources when the function is finished. In this model, you're only charged for the CPU time used while your function runs.

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

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

[Continue](#)

Need help? See our troubleshooting guide or provide specific feedback by reporting an issue .

[Describe application hosting options](#)

Completed

- 3 minutes

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, Twitter, and Facebook.
- Send push notifications.
- Execute custom back-end logic in C# or Node.js.

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

[Continue](#)

Need help? See our troubleshooting guide or provide specific feedback by reporting an issue .

[Describe Azure virtual networking](#)

Completed

- 5 minutes

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 that's 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'll 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, which 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.

[Continue](#)

Need help? See our troubleshooting guide or provide specific feedback by reporting an issue .

Exercise - Configure network access

Completed

- 10 minutes

In this exercise, you'll 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:

```
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, the VM you created and installed Nginx on isn't accessible from the internet. You'll create a network security group that changes that by allowing inbound HTTP access on port 80.

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:

```
IPADDRESS="$(az vm list-ip-addresses \
  --resource-group <rgn>[sandbox resource group name]</rgn> \
  --name my-vm \
  --query "[].virtualMachine.network.publicIpAddresses[*].ipAddress" \
  --output tsv)"
```

2. Run the following `curl` command to download the home page:

```
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:

```
curl: (28) Connection timed out after 5001 milliseconds
```

This message means that the VM was not accessible within the timeout period.

3. As an optional step, try to access the web server from a browser:

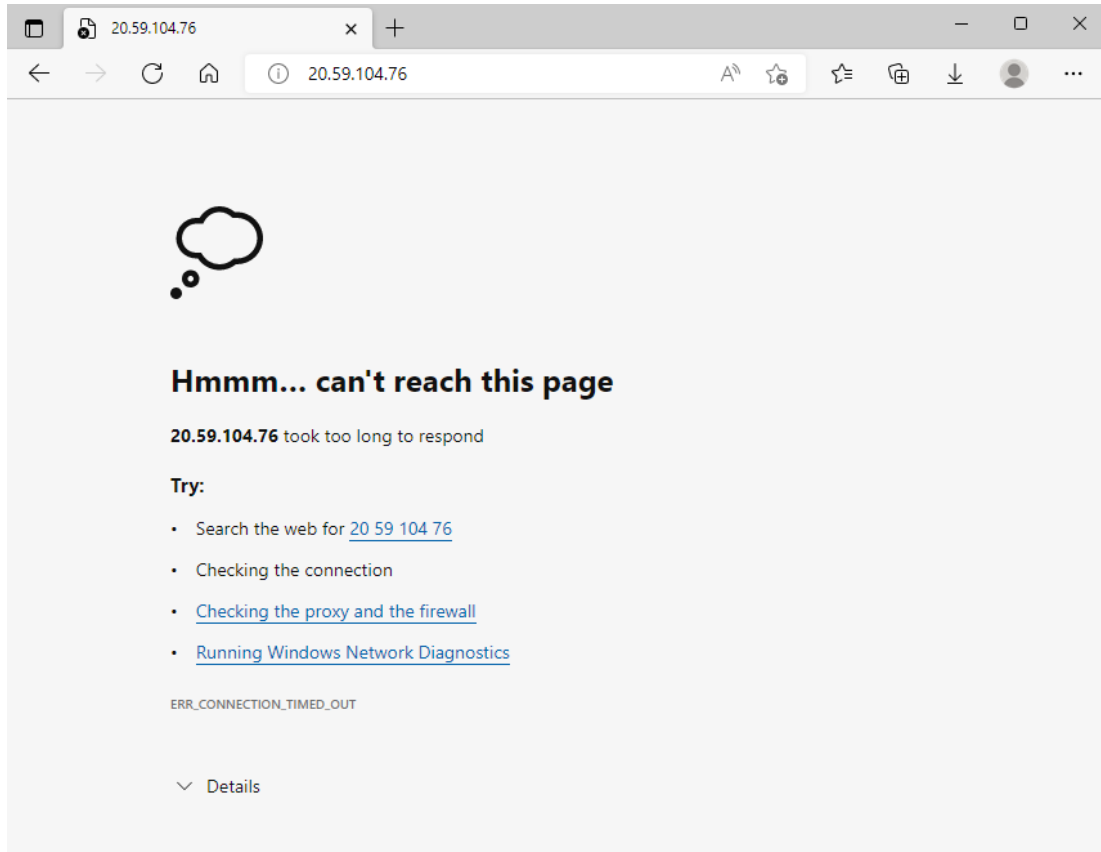
1. Run the following to print your VM's IP address to the console:

```
echo $IPADDRESS
```

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

2. Copy the IP address that you see to the clipboard.
3. Open a new browser tab and go to your web server. After a few moments, you see that the connection isn't happening.

If you wait for the browser to time out, you'll see something like this:



4. 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:

```
az network nsg list \
  --resource-group <rgn>[sandbox resource group name]</rgn> \
  --query '[] .name' \
  --output tsv
```

You see this:

```
my-vmNSG
```

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

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

```
az network nsg rule list \
  --resource-group <rgn>[sandbox resource group name]</rgn> \
```

```
--nsg-name my-vmNSG
```

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

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

```
az network nsg rule list \
--resource-group <rgn>[sandbox resource group name]</rgn> \
--nsg-name my-vmNSG \
--query '[Name:name, Priority:priority, Port:destinationPortRange, Access:access]' \
--output table
```

You see this:

Name	Priority	Port	Access
default-allow-ssh	1000	22	Allow

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

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

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:

```
az network nsg rule create \
--resource-group <rgn>[sandbox resource group name]</rgn> \
--nsg-name my-vmNSG \
--name allow-http \
--protocol tcp \
--priority 100 \
--destination-port-range 80 \
--access Allow
```

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

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

```
az network nsg rule list \
--resource-group <rgn>[sandbox resource group name]</rgn> \
--nsg-name my-vmNSG \
--query '[Name:name, Priority:priority, Port:destinationPortRange, Access:access]' \
```

```
--output table
```

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

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've 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:

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

You see this:

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

2. As an optional step, refresh your browser tab that points to your web server.

You see this:



Welcome to Azure! My name is my-vm.

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.

[Continue](#)

Need help? See our troubleshooting guide or provide specific feedback by reporting an issue .

[Describe Azure virtual private networks](#)

Completed

- 5 minutes

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 pre-shared 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're typically restored within a few seconds for planned maintenance and within 90 seconds for unplanned disruptions.

Active/active

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

ExpressRoute failover

Another high-availability option is to configure a VPN gateway as a secure failover path for ExpressRoute connections. ExpressRoute circuits have resiliency built in. 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.

[Continue](#)

Need help? See our troubleshooting guide or provide specific feedback by reporting an issue .

[Describe Azure ExpressRoute](#)

Completed

- 4 minutes

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

datacenters, or other facilities to the Microsoft cloud. Each location would have its own ExpressRoute circuit.

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

Features and benefits of ExpressRoute

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

- Connectivity to Microsoft cloud services across all regions in the geopolitical region.
- Global connectivity to Microsoft services across all regions with the ExpressRoute Global Reach.
- Dynamic routing between your network and Microsoft via Border Gateway Protocol (BGP).
- Built-in redundancy in every peering location for higher reliability.

Connectivity to Microsoft cloud services

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

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

Global connectivity

You can enable ExpressRoute Global Reach to exchange data across your on-premises sites by connecting your ExpressRoute circuits. For example, say you had an office in Asia and a datacenter in Europe, both with ExpressRoute circuits connecting them to the Microsoft network. You could use ExpressRoute Global Reach to connect those two facilities, allowing them to communicate without transferring data over the public internet.

Dynamic routing

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

Built-in redundancy

Each connectivity provider uses redundant devices to ensure that connections established with Microsoft are highly available. You can configure multiple circuits to complement this feature.

ExpressRoute connectivity models

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

- CloudExchange colocation
- Point-to-point Ethernet connection
- Any-to-any connection
- Directly from ExpressRoute sites

Co-location at a cloud exchange

Co-location refers to your datacenter, office, or other facility being physically co-located at a cloud exchange, such as an ISP. If your facility is co-located at a cloud exchange, you can request a virtual cross-connect to the Microsoft cloud.

Point-to-point Ethernet connection

Point-to-point ethernet connection refers to using a point-to-point connection to connect your facility to the Microsoft cloud.

Any-to-any networks

With any-to-any connectivity, you can integrate your wide area network (WAN) with Azure by providing connections to your offices and datacenters. Azure integrates with your WAN connection to provide a connection like you would have between your datacenter and any branch offices.

Directly from ExpressRoute sites

You can connect directly into the Microsoft's global network at a peering location strategically distributed across the world. ExpressRoute Direct provides dual 100 Gbps or 10-Gbps connectivity, which supports Active/Active connectivity at scale.

Security considerations

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

[Continue](#)

Need help? See our troubleshooting guide or provide specific feedback by reporting an issue .

[Describe Azure DNS](#)

Completed

- 3 minutes

Azure DNS is a hosting service for DNS domains that provides name resolution by using Microsoft Azure infrastructure. By hosting your domains in Azure, you can manage your DNS records using the same credentials, APIs, tools, and billing as your other Azure services.

Benefits of Azure DNS

Azure DNS leverages the scope and scale of Microsoft Azure to provide numerous benefits, including:

- Reliability and performance
- Security
- Ease of Use
- Customizable virtual networks
- Alias records

Reliability and performance

DNS domains in Azure DNS are hosted on Azure's global network of DNS name servers, providing resiliency and high availability. Azure DNS uses anycast networking, so each DNS query is answered by the closest available DNS server to provide fast performance and high availability for your domain.

Security

Azure DNS is based on Azure Resource Manager, which provides features such as:

- Azure role-based access control (Azure RBAC) to control who has access to specific actions for your organization.
- Activity logs to monitor how a user in your organization modified a resource or to find an error when troubleshooting.
- Resource locking to lock a subscription, resource group, or resource. Locking prevents other users in your organization from accidentally deleting or modifying critical resources.

Ease of use

Azure DNS can manage DNS records for your Azure services and provide DNS for your external resources as well. Azure DNS is integrated in the Azure portal and uses the same credentials, support contract, and billing as your other Azure services.

Because Azure DNS is running on Azure, it means you can manage your domains and records with the Azure portal, Azure PowerShell cmdlets, and the cross-platform Azure CLI. Applications that require automated DNS management can integrate with the service by using the REST API and SDKs.

Customizable virtual networks with private domains

Azure DNS also supports private DNS domains. This feature allows you to use your own custom domain names in your private virtual networks, rather than being stuck with the Azure-provided names.

Alias records

Azure DNS also supports alias record sets. You can use an alias record set to refer to an Azure resource, such as an Azure public IP address, an Azure Traffic Manager profile, or an Azure Content Delivery Network (CDN) endpoint. If the IP address of the underlying resource changes, the alias record set seamlessly updates itself during DNS resolution. The alias record set points to the service instance, and the service instance is associated with an IP address.

Important

You can't use Azure DNS to buy a domain name. For an annual fee, you can buy a domain name by using App Service domains or a third-party domain name registrar. Once purchased, your domains can be hosted in Azure DNS for record management.

[Continue](#)

Need help? See our troubleshooting guide or provide specific feedback by reporting an issue .

[Knowledge check](#)

Completed

- 4 minutes

Choose the best response for each question. Then select **Check your answers** .

Check your knowledge

1.

Which Azure Virtual Machine feature staggers updates across VMs based on their update domain and fault domain?

☐

Availability sets

☐

Scale sets

☐

Update sets

2.

Which Azure service allows users to use a cloud hosted version of Windows from any location and connect from most modern browsers?

☐

Azure Virtual Desktop

☐

Azure Virtual Machines

☐

Azure Container Instances

Check your answers

You must answer all questions before checking your work.

[Continue](#)

Need help? See our troubleshooting guide or provide specific feedback by reporting an issue .

Summary

Completed

- 2 minutes

In this module, you learned about some of the compute and networking services that are part of Azure. You learned about virtual machines, and the different options associated with them (such as virtual machine scale sets and virtual machine availability sets). You were also introduced to some of the networking capabilities, including virtual networking, ExpressRoute, and virtual private networks.

Learning objectives

You should now 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.

Additional resources

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

- [Host a web application with Azure App Service](#) is a Microsoft Learn module that explores the process of hosting a web application in Azure.
- [Introduction to Azure network foundation services](#) is a Microsoft Learn course that provides greater insight and information on networking with Azure.

[Continue](#)

Need help? See our troubleshooting guide or provide specific feedback by reporting an issue .

Describe Azure storage services

Introduction

Completed

- 1 minute

In this module, you'll be introduced to the Azure storage services. You'll learn about the Azure Storage Account and how that relates to the different storage services that are available. You'll also learn about blob storage tiers, data redundancy options, and ways to move data or even entire infrastructures to Azure.

Learning objectives

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

- Compare Azure storage services.
- Describe storage tiers.
- Describe redundancy options.
- Describe storage account options and storage types.
- Identify options for moving files, including AzCopy, Azure Storage Explorer, and Azure File Sync.
- Describe migration options, including Azure Migrate and Azure Data Box.

[Continue](#)

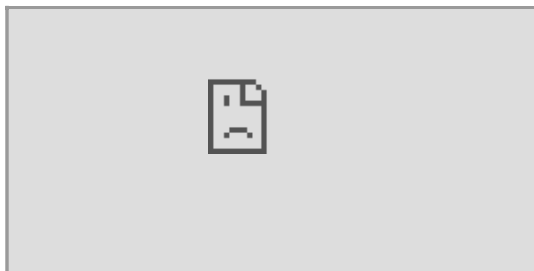
Need help? See our troubleshooting guide or provide specific feedback by reporting an issue .

Describe Azure storage accounts

Completed

- 5 minutes

The following video introduces the different services that should be available with Azure Storage.



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

When you create your storage account, you'll start by picking the storage account type. The type of account determines the storage services and redundancy options and has an impact on the use cases. Below is a list of redundancy options that will be covered later in this module:

- Locally redundant storage (LRS)
- Geo-redundant storage (GRS)
- Read-access geo-redundant storage (RA-GRS)
- Zone-redundant storage (ZRS)
- Geo-zone-redundant storage (GZRS)
- Read-access geo-zone-redundant storage (RA-GZRS)

Type	Supported services	Redundancy Options	Usage
Standard general-purpose v2	Blob Storage (including Data Lake Storage), Queue Storage, Table Storage, and Azure Files	LRS, GRS, RA-GRS, ZRS, GZRS, RA-GZRS	Standard storage account type for blobs, file shares, queues, and tables. Recommended for most scenarios using Azure Storage. If you want support for network file system (NFS) in Azure Files, use the premium file shares account type.
Premium block blobs	Blob Storage (including Data Lake Storage)	LRS, ZRS	Premium storage account type for block blobs and append blobs. Recommended for scenarios with high transaction rates or that use smaller objects or require consistently low storage latency.
Premium file shares	Azure Files	LRS, ZRS	Premium storage account type for file shares only. Recommended for enterprise or high-performance scale applications. Use this account type if you want a storage account that supports both Server Message Block (SMB) and NFS file shares.
Premium page blobs	Page blobs only	LRS	Premium storage account type for page blobs only.

Storage account endpoints

One of the benefits of using an Azure Storage Account is having a unique namespace in Azure for your data. In order to do this, every storage account in Azure must have a unique-in-Azure account name. The combination of the account name and the Azure Storage service endpoint forms the endpoints for your storage account.

When naming your storage account, keep these rules in mind:

- Storage account names must be between 3 and 24 characters in length and may contain numbers and lowercase letters only.
- Your storage account name must be unique within Azure. No two storage accounts can have the same name. This supports the ability to have a unique, accessible namespace in

Azure.

The following table shows the endpoint format for Azure Storage services.

Storage service	Endpoint
Blob Storage	https://<storage-account-name>.blob.core.windows.net
Data Lake Storage Gen2	https://<storage-account-name>.dfs.core.windows.net
Azure Files	https://<storage-account-name>.file.core.windows.net
Queue Storage	https://<storage-account-name>.queue.core.windows.net
Table Storage	https://<storage-account-name>.table.core.windows.net

[Continue](#)

Need help? See our troubleshooting guide or provide specific feedback by reporting an issue .

[Describe Azure storage redundancy](#)

Completed

- 6 minutes

Azure Storage always stores multiple copies of your data so that it's protected from planned and unplanned events such as transient hardware failures, network or power outages, and natural disasters. Redundancy ensures that your storage account meets its availability and durability targets even in the face of failures.

When deciding which redundancy option is best for your scenario, consider the tradeoffs between lower costs and higher availability. The factors that help determine which redundancy option you should choose include:

- How your data is replicated in the primary region.
- Whether your data is replicated to a second region that is geographically distant to the primary region, to protect against regional disasters.
- Whether your application requires read access to the replicated data in the secondary region if the primary region becomes unavailable.

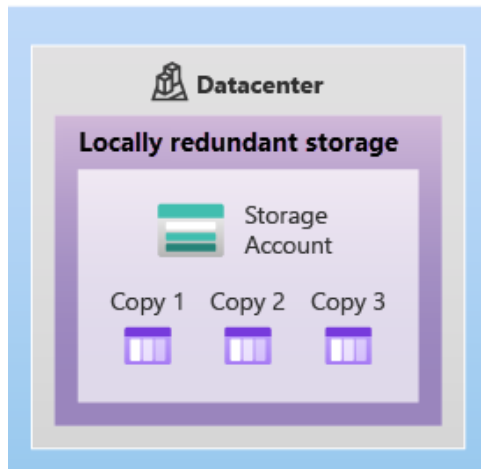
Redundancy in the primary region

Data in an Azure Storage account is always replicated three times in the primary region. Azure Storage offers two options for how your data is replicated in the primary region, locally redundant storage (LRS) and zone-redundant storage (ZRS).

Locally redundant storage

Locally redundant storage (LRS) replicates your data three times within a single data center in the primary region. LRS provides at least 11 nines of durability (99.999999999%) of objects over a given year.

Primary region

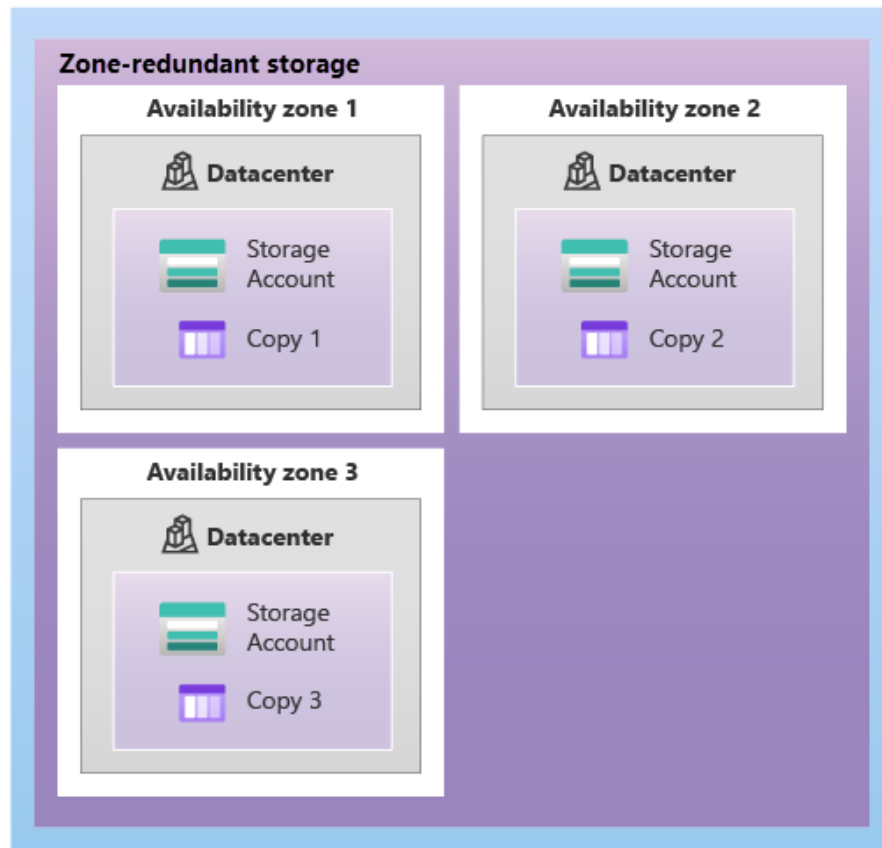


LRS is the lowest-cost redundancy option and offers the least durability compared to other options. LRS protects your data against server rack and drive failures. However, if a disaster such as fire or flooding occurs within the data center, all replicas of a storage account using LRS may be lost or unrecoverable. To mitigate this risk, Microsoft recommends using zone-redundant storage (ZRS), geo-redundant storage (GRS), or geo-zone-redundant storage (GZRS).

Zone-redundant storage

For Availability Zone-enabled Regions, zone-redundant storage (ZRS) replicates your Azure Storage data synchronously across three Azure availability zones in the primary region. ZRS offers durability for Azure Storage data objects of at least 12 nines (99.999999999%) over a given year.

Primary region



With ZRS, your data is still accessible for both read and write operations even if a zone becomes unavailable. No remounting of Azure file shares from the connected clients is required. If a zone becomes unavailable, Azure undertakes networking updates, such as DNS repointing. These updates may affect your application if you access data before the updates have completed.

Microsoft recommends using ZRS in the primary region for scenarios that require high availability. ZRS is also recommended for restricting replication of data within a country or region to meet data governance requirements.

Redundancy in a secondary region

For applications requiring high durability, you can choose to additionally copy the data in your storage account to a secondary region that is hundreds of miles away from the primary region. If the data in your storage account is copied to a secondary region, then your data is durable even in the event of a catastrophic failure that prevents the data in the primary region from being recovered.

When you create a storage account, you select the primary region for the account. The paired secondary region is based on Azure Region Pairs, and can't be changed.

Azure Storage offers two options for copying your data to a secondary region: geo-redundant storage (GRS) and geo-zone-redundant storage (GZRS). GRS is similar to running LRS in two

regions, and GZRS is similar to running ZRS in the primary region and LRS in the secondary region.

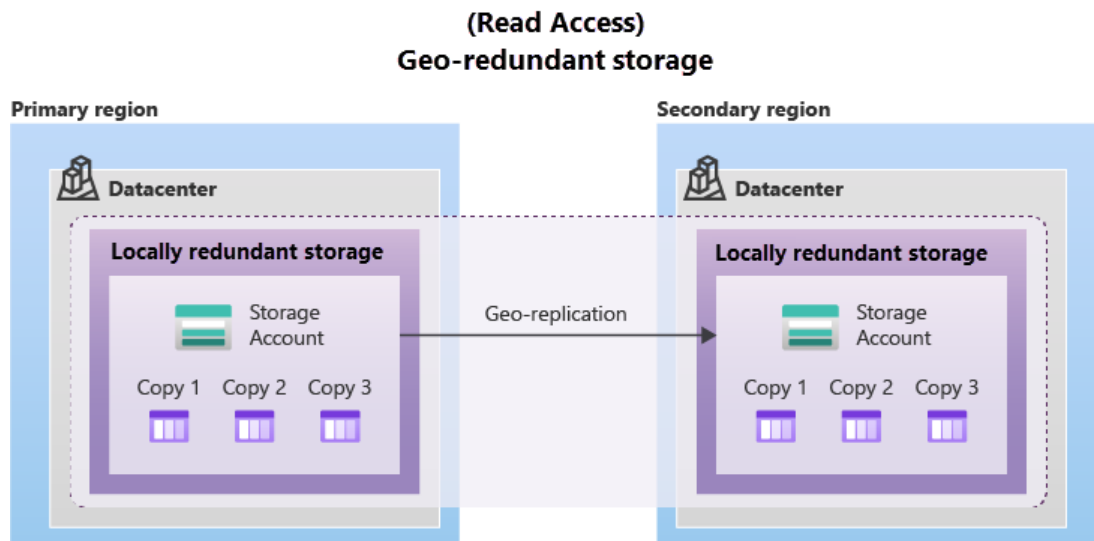
By default, data in the secondary region isn't available for read or write access unless there's a failover to the secondary region. If the primary region becomes unavailable, you can choose to fail over to the secondary region. After the failover has completed, the secondary region becomes the primary region, and you can again read and write data.

Important

Because data is replicated to the secondary region asynchronously, a failure that affects the primary region may result in data loss if the primary region can't be recovered. The interval between the most recent writes to the primary region and the last write to the secondary region is known as the recovery point objective (RPO). The RPO indicates the point in time to which data can be recovered. Azure Storage typically has an RPO of less than 15 minutes, although there's currently no SLA on how long it takes to replicate data to the secondary region.

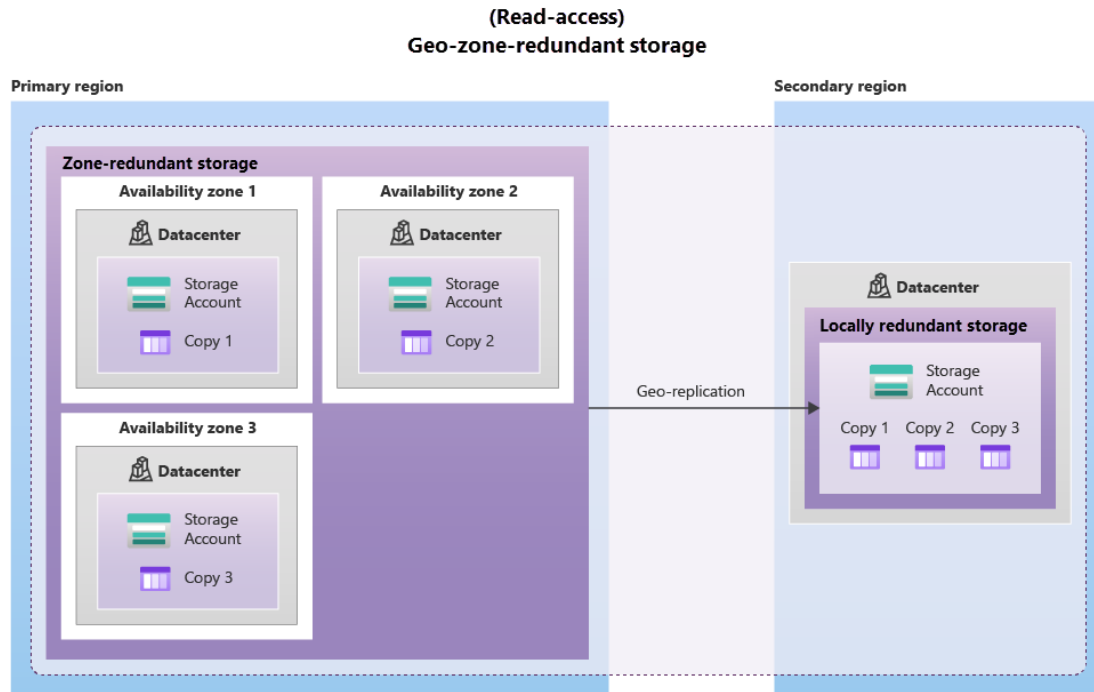
Geo-redundant storage

GRS copies your data synchronously three times within a single physical location in the primary region using LRS. It then copies your data asynchronously to a single physical location in the secondary region (the region pair) using LRS. GRS offers durability for Azure Storage data objects of at least 16 nines (99.9999999999999%) over a given year.



Geo-zone-redundant storage

GZRS combines the high availability provided by redundancy across availability zones with protection from regional outages provided by geo-replication. Data in a GZRS storage account is copied across three Azure availability zones in the primary region (similar to ZRS) and is also replicated to a secondary geographic region, using LRS, for protection from regional disasters. Microsoft recommends using GZRS for applications requiring maximum consistency, durability, and availability, excellent performance, and resilience for disaster recovery.



GZRS is designed to provide at least 16 nines (99.99999999999999%) of durability of objects over a given year.

Read access to data in the secondary region

Geo-redundant storage (with GRS or GZRS) replicates your data to another physical location in the secondary region to protect against regional outages. However, that data is available to be read only if the customer or Microsoft initiates a failover from the primary to secondary region. However, if you enable read access to the secondary region, your data is always available, even when the primary region is running optimally. For read access to the secondary region, enable read-access geo-redundant storage (RA-GRS) or read-access geo-zone-redundant storage (RA-GZRS).

Important

Remember that the data in your secondary region may not be up-to-date due to RPO.

[Continue](#)

Need help? See our troubleshooting guide or provide specific feedback by reporting an issue .

[Describe Azure storage services](#)

Completed

- 10 minutes

The Azure Storage platform includes the following data services:

- **Azure Blobs** : A massively scalable object store for text and binary data. Also includes support for big data analytics through Data Lake Storage Gen2.
- **Azure Files** : Managed file shares for cloud or on-premises deployments.
- **Azure Queues** : A messaging store for reliable messaging between application components.
- **Azure Disks** : Block-level storage volumes for Azure VMs.
- **Azure Tables**: NoSQL table option for structured, non-relational data.

Benefits of Azure Storage

Azure Storage services offer the following benefits for application developers and IT professionals:

- **Durable and highly available** . Redundancy ensures that your data is safe if transient hardware failures occur. You can also opt to replicate data across data centers or geographical regions for additional protection from local catastrophes or natural disasters. Data replicated in this way remains highly available if an unexpected outage occurs.
- **Secure** . All data written to an Azure storage account is encrypted by the service. Azure Storage provides you with fine-grained control over who has access to your data.
- **Scalable** . Azure Storage is designed to be massively scalable to meet the data storage and performance needs of today's applications.
- **Managed** . Azure handles hardware maintenance, updates, and critical issues for you.
- **Accessible** . Data in Azure Storage is accessible from anywhere in the world over HTTP or HTTPS. Microsoft provides client libraries for Azure Storage in a variety of languages, including .NET, Java, Node.js, Python, PHP, Ruby, Go, and others, as well as a mature REST API. Azure Storage supports scripting in Azure PowerShell or Azure CLI. And the Azure portal and Azure Storage Explorer offer easy visual solutions for working with your data.

Azure Blobs

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

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

Blob storage is ideal for:

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

Accessing blob storage

Objects in blob storage can be accessed from anywhere in the world via HTTP or HTTPS. Users or client applications can access blobs via URLs, the Azure Storage REST API, Azure PowerShell, Azure CLI, or an Azure Storage client library. The storage client libraries are available for multiple languages, including .NET, Java, Node.js, Python, PHP, and Ruby.

Blob storage tiers

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

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

- **Hot access tier** : Optimized for storing data that is accessed frequently (for example, images for your website).
- **Cool access tier** : Optimized for data that is infrequently accessed and stored for at least 30 days (for example, invoices for your customers).
- **Cold access tier** : Optimized for storing data that is infrequently accessed and stored for at least 90 days.
- **Archive access tier** : Appropriate for data that is rarely accessed and stored for at least 180 days, with flexible latency requirements (for example, long-term backups).

The following considerations apply to the different access tiers:

- Hot, cool, and cold access tiers can be set at the account level. The archive access tier isn't available at the account level.
- Hot, cool, cold, and archive tiers can be set at the blob level, during or after upload.
- Data in the cool and cold access tiers can tolerate slightly lower availability, but still requires high durability, retrieval latency, and throughput characteristics similar to hot data. For cool and cold data, a lower availability service-level agreement (SLA) and higher access costs compared to hot data are acceptable trade-offs for lower storage costs.
- Archive storage stores data offline and offers the lowest storage costs, but also the highest costs to rehydrate and access data.

Azure Files

Azure File storage offers fully managed file shares in the cloud that are accessible via the industry standard Server Message Block (SMB) or Network File System (NFS) protocols. Azure Files file shares can be mounted concurrently by cloud or on-premises deployments. SMB Azure file shares are accessible from Windows, Linux, and macOS clients. NFS Azure Files shares are

accessible from Linux or macOS clients. Additionally, SMB Azure file shares can be cached on Windows Servers with Azure File Sync for fast access near where the data is being used.

Azure Files key benefits:

- **Shared access** : Azure file shares support the industry standard SMB and NFS protocols, meaning you can seamlessly replace your on-premises file shares with Azure file shares without worrying about application compatibility.
- **Fully managed** : Azure file shares can be created without the need to manage hardware or an OS. This means you don't have to deal with patching the server OS with critical security upgrades or replacing faulty hard disks.
- **Scripting and tooling** : PowerShell cmdlets and Azure CLI can be used to create, mount, and manage Azure file shares as part of the administration of Azure applications. You can create and manage Azure file shares using Azure portal and Azure Storage Explorer.
- **Resiliency** : Azure Files has been built from the ground up to always be available. Replacing on-premises file shares with Azure Files means you don't have to wake up in the middle of the night to deal with local power outages or network issues.
- **Familiar programmability** : Applications running in Azure can access data in the share via file system I/O APIs. Developers can therefore use their existing code and skills to migrate existing applications. In addition to System IO APIs, you can use Azure Storage Client Libraries or the Azure Storage REST API.

Azure Queues

Azure Queue storage is a service for storing large numbers of messages. Once stored, you can access the messages from anywhere in the world via authenticated calls using HTTP or HTTPS. A queue can contain as many messages as your storage account has room for (potentially millions). Each individual message can be up to 64 KB in size. Queues are commonly used to create a backlog of work to process asynchronously.

Queue storage can be combined with compute functions like Azure Functions to take an action when a message is received. For example, you want to perform an action after a customer uploads a form to your website. You could have the submit button on the website trigger a message to the Queue storage. Then, you could use Azure Functions to trigger an action once the message was received.

Azure Disks

Azure Disk storage, or Azure managed disks, are block-level storage volumes managed by Azure for use with Azure VMs. Conceptually, they're the same as a physical disk, but they're virtualized – offering greater resiliency and availability than a physical disk. With managed disks, all you have to do is provision the disk, and Azure will take care of the rest.

Azure Tables

Azure Table storage stores large amounts of structured data. Azure tables are a NoSQL datastore that accepts authenticated calls from inside and outside the Azure cloud. This enables you to use Azure tables to build your hybrid or multi-cloud solution and have your data always available. Azure tables are ideal for storing structured, non-relational data.

[Continue](#)

Need help? See our troubleshooting guide or provide specific feedback by reporting an issue .

Exercise - Create a storage blob

Completed

- 10 minutes

Create a storage account

In this task, you'll create a new storage account.

1. Sign in to the Azure portal at <https://portal.azure.com>
2. Select **Create a resource** .
3. Under Categories, select **Storage** .
4. Under Storage account, select **Create** .
5. On the **Basics** tab of the Create a storage account blade, fill in the following information. Leave the defaults for everything else.

Setting	Value
Subscription	Concierge Subscription
Resource group	Select the resource group that starts with learn
Storage account name	Create a unique storage account name
Region	Leave default
Performance	Standard
Redundancy	Locally redundant storage (LRS)

6. On the **Advanced** tab of the Create a storage account blade, fill in the following information. Leave the defaults for everything else.

Setting	Value
Allow enabling anonymous access on individual containers	Checked

Security

Configure security settings that impact your storage account.

Require secure transfer for REST API operations ⓘ ☒

Allow enabling anonymous access on individual containers ⓘ ☒

Enable storage account key access ⓘ ☒

Default to Azure Active Directory authorization in the Azure portal ⓘ ☐

Minimum TLS version ⓘ Version 1.2 ▼

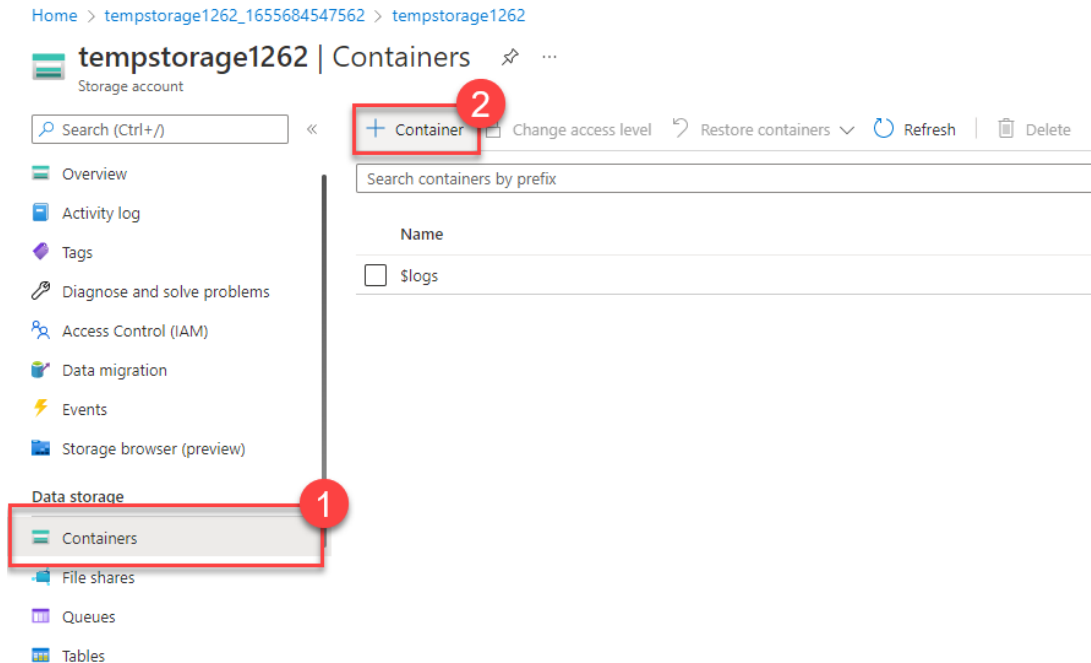
Permitted scope for copy operations (preview) ⓘ From any storage account ▼

7. Select **Review** to review your storage account settings and allow Azure to validate the configuration.
8. Once validated, select **Create** . Wait for the notification that the account was successfully created.
9. Select **Go to resource** .

Work with blob storage

In this section, you'll create a Blob container and upload a picture.

1. Under **Data storage** , select **Containers** .



2. Select **+ Container** and complete the information.

Setting	Value
Name	Enter a name for the container
Public access level	Private (no anonymous access)

3. Select Create.

Note

Step 4 will need an image. If you want to upload an image you already have on your computer, continue to Step 4. Otherwise, open a new browser window and search Bing for an image of a flower. Save the image to your computer.

4. Back in the Azure portal, select the container you created, then select Upload.

5. Browse for the image file you want to upload. Select it and then select upload.

Note

You can upload as many blobs as you like in this way. New blobs will be listed within the container.

6. Select the Blob (file) you just uploaded. You should be on the properties tab.

7. Copy the URL from the URL field and paste it into a new tab.

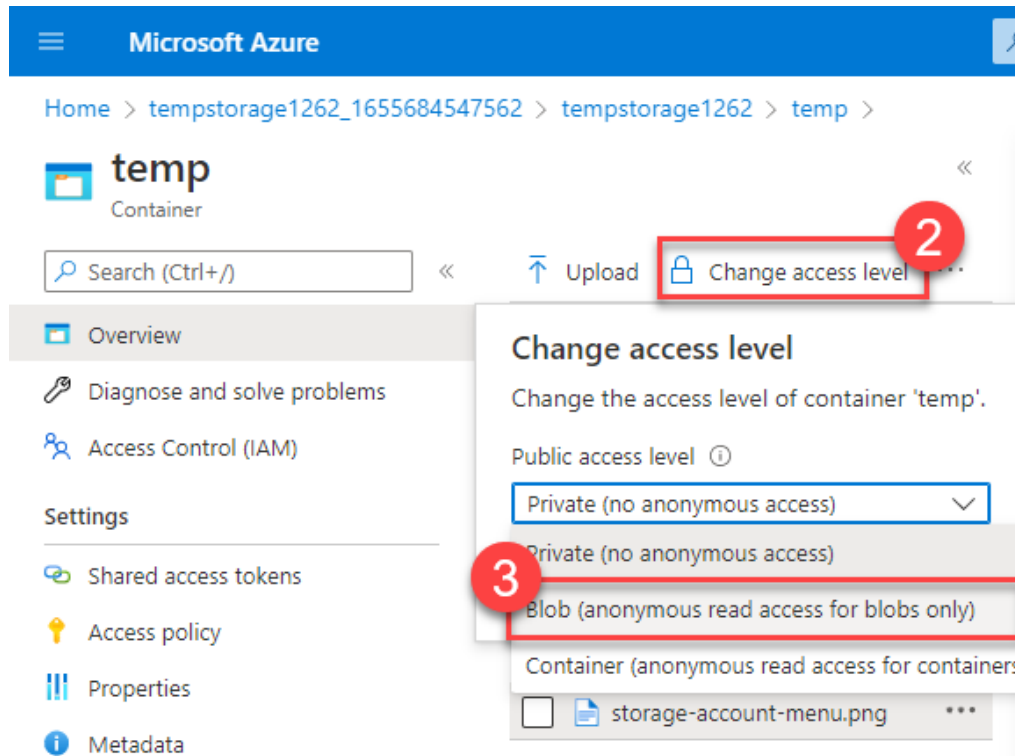
You should receive an error message similar to the following.

```
<Error>
  <Code>ResourceNotFound</Code>
  <Message>The specified resource does not exist. RequestId:4a4bd3d9-101e-005a-1a3e-
```

84bd42000000</Message>
</Error>

Change the access level of your blob

1. Go back to the Azure portal.
2. Select Change access level.
3. Set the Public access level to Blob (anonymous read access for blobs only).



4. Select OK.
5. Refresh the tab where you attempted to access the file earlier.

Congratulations - you've completed this exercise. You created a storage account, added a container to the storage account, and then uploaded blobs (files) to your container. Then you changed the access level so you could access your file from the internet.

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.

[Continue](#)

Need help? See our troubleshooting guide or provide specific feedback by reporting an issue .

Identify Azure data migration options

Completed

- 5 minutes

Now that you understand the different storage options within Azure, it's important to also understand how to get your data and information into Azure. Azure supports both real-time migration of infrastructure, applications, and data using Azure Migrate as well as asynchronous migration of data using Azure Data Box.

Azure Migrate

Azure Migrate is a service that helps you migrate from an on-premises environment to the cloud. Azure Migrate functions as a hub to help you manage the assessment and migration of your on-premises datacenter to Azure. It provides the following:

- **Unified migration platform** : A single portal to start, run, and track your migration to Azure.
- **Range of tools** : A range of tools for assessment and migration. Azure Migrate tools include Azure Migrate: Discovery and assessment and Azure Migrate: Server Migration. Azure Migrate also integrates with other Azure services and tools, and with independent software vendor (ISV) offerings.
- **Assessment and migration** : In the Azure Migrate hub, you can assess and migrate your on-premises infrastructure to Azure.

Integrated tools

In addition to working with tools from ISVs, the Azure Migrate hub also includes the following tools to help with migration:

- **Azure Migrate: Discovery and assessment** . Discover and assess on-premises servers running on VMware, Hyper-V, and physical servers in preparation for migration to Azure.
- **Azure Migrate: Server Migration** . Migrate VMware VMs, Hyper-V VMs, physical servers, other virtualized servers, and public cloud VMs to Azure.
- **Data Migration Assistant** . Data Migration Assistant is a stand-alone tool to assess SQL Servers. It helps pinpoint potential problems blocking migration. It identifies unsupported features, new features that can benefit you after migration, and the right path for database migration.
- **Azure Database Migration Service** . Migrate on-premises databases to Azure VMs running SQL Server, Azure SQL Database, or SQL Managed Instances.
- **Azure App Service migration assistant** . Azure App Service migration assistant is a standalone tool to assess on-premises websites for migration to Azure App Service. Use Migration Assistant to migrate .NET and PHP web apps to Azure.

- **Azure Data Box** . Use Azure Data Box products to move large amounts of offline data to Azure.

Azure Data Box

Azure Data Box is a physical migration service that helps transfer large amounts of data in a quick, inexpensive, and reliable way. The secure data transfer is accelerated by shipping you a proprietary Data Box storage device that has a maximum usable storage capacity of 80 terabytes. The Data Box is transported to and from your datacenter via a regional carrier. A rugged case protects and secures the Data Box from damage during transit.

You can order the Data Box device via the Azure portal to import or export data from Azure. Once the device is received, you can quickly set it up using the local web UI and connect it to your network. Once you're finished transferring the data (either into or out of Azure), simply return the Data Box. If you're transferring data into Azure, the data is automatically uploaded once Microsoft receives the Data Box back. The entire process is tracked end-to-end by the Data Box service in the Azure portal.

Use cases

Data Box is ideally suited to transfer data sizes larger than 40 TBs in scenarios with no to limited network connectivity. The data movement can be one-time, periodic, or an initial bulk data transfer followed by periodic transfers.

Here are the various scenarios where Data Box can be used to import data to Azure.

- Onetime migration - when a large amount of on-premises data is moved to Azure.
- Moving a media library from offline tapes into Azure to create an online media library.
- Migrating your VM farm, SQL server, and applications to Azure.
- Moving historical data to Azure for in-depth analysis and reporting using HDInsight.
- Initial bulk transfer - when an initial bulk transfer is done using Data Box (seed) followed by incremental transfers over the network.
- Periodic uploads - when large amount of data is generated periodically and needs to be moved to Azure.

Here are the various scenarios where Data Box can be used to export data from Azure.

- Disaster recovery - when a copy of the data from Azure is restored to an on-premises network. In a typical disaster recovery scenario, a large amount of Azure data is exported to a Data Box. Microsoft then ships this Data Box, and the data is restored on your premises in a short time.
- Security requirements - when you need to be able to export data out of Azure due to government or security requirements.
- Migrate back to on-premises or to another cloud service provider - when you want to move all the data back to on-premises, or to another cloud service provider, export data via Data Box to migrate the workloads.

Once the data from your import order is uploaded to Azure, the disks on the device are wiped clean in accordance with NIST 800-88r1 standards. For an export order, the disks are erased once the device reaches the Azure datacenter.

[Continue](#)

Need help? See our troubleshooting guide or provide specific feedback by reporting an issue .

Identify Azure file movement options

Completed

- 3 minutes

In addition to large scale migration using services like Azure Migrate and Azure Data Box, Azure also has tools designed to help you move or interact with individual files or small file groups.

Among those tools are AzCopy, Azure Storage Explorer, and Azure File Sync.

AzCopy

AzCopy is a command-line utility that you can use to copy blobs or files to or from your storage account. With AzCopy, you can upload files, download files, copy files between storage accounts, and even synchronize files. AzCopy can even be configured to work with other cloud providers to help move files back and forth between clouds.

Important

Synchronizing blobs or files with AzCopy is one-direction synchronization. When you synchronize, you designated the source and destination, and AzCopy will copy files or blobs in that direction. It doesn't synchronize bi-directionally based on timestamps or other metadata.

Azure Storage Explorer

Azure Storage Explorer is a standalone app that provides a graphical interface to manage files and blobs in your Azure Storage Account. It works on Windows, macOS, and Linux operating systems and uses AzCopy on the backend to perform all of the file and blob management tasks. With Storage Explorer, you can upload to Azure, download from Azure, or move between storage accounts.

Azure File Sync

Azure File Sync is a tool that lets you centralize your file shares in Azure Files and keep the flexibility, performance, and compatibility of a Windows file server. It's almost like turning your Windows file server into a miniature content delivery network. Once you install Azure File Sync on your local Windows server, it will automatically stay bi-directionally synced with your files in Azure.

With Azure File Sync, you can:

- Use any protocol that's available on Windows Server to access your data locally, including SMB, NFS, and FTPS.
- Have as many caches as you need across the world.
- Replace a failed local server by installing Azure File Sync on a new server in the same datacenter.

- Configure cloud tiering so the most frequently accessed files are replicated locally, while infrequently accessed files are kept in the cloud until requested.

[Continue](#)

Need help? See our troubleshooting guide or provide specific feedback by reporting an issue .

[Knowledge check](#)

Completed

- 4 minutes

Choose the best response for each question. Then select **Check your answers** .

Check your knowledge

1.

Which tool automatically keeps files between an on-premises Windows server and an Azure cloud environment updated?

☐

Azure File Sync

☐

Azure Storage Explorer

☐

AzCopy

2.

Which storage redundancy option provides the highest degree of durability, with 16 nines of durability?

☐

Locally redundant storage

☐

Zone-redundant storage

☐

Geo-zone-redundant-storage

3.

Which Azure Storage service supports big data analytics, as well as handling text and binary data types?

☐

Azure Blobs

☐

Azure Files

☐

Azure Disks

Check your answers

You must answer all questions before checking your work.

[Continue](#)

Need help? See our troubleshooting guide or provide specific feedback by reporting an issue .

Summary

Completed

- 2 minutes

In this module, you learned about the Azure storage services. You learned about the Azure Storage Account and how they relate to different storage services. You were introduced to storage blobs and redundancy options, and ways to migrate and move your data both into and within Azure.

Learning objectives

You should now be able to:

- Compare Azure storage services.
- Describe storage tiers.
- Describe redundancy options.
- Describe storage account options and storage types.
- Identify options for moving files, including AzCopy, Azure Storage Explorer, and Azure File Sync.
- Describe migration options, including Azure Migrate and Azure Data Box.

Additional resources

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

- [Store data in Azure](#) is a Microsoft Learn course that covers more information about storing data in Azure.
- [Microsoft Certified: Azure Data Fundamentals](#) is an entire certification, with associated training that dives deeper into data fundamentals on Azure.

[Continue](#)

Need help? See our troubleshooting guide or provide specific feedback by reporting an issue .

Describe Azure identity, access, and security

Introduction

Completed

- 1 minute

In this module, you'll be introduced to the Azure identity, access, and security services and tools. You'll learn about directory services in Azure, authentication methods, and access control. You'll also cover things like Zero Trust and defense in depth, and how they keep your cloud safer. You'll wrap up with an introduction to Microsoft Defender for Cloud.

Learning objectives

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

- Describe directory services in Azure, including Microsoft Entra ID and Microsoft Entra Domain Services.
- Describe authentication methods in Azure, including single sign-on (SSO), multifactor authentication (MFA), and passwordless.
- Describe external identities and guest access in Azure.
- Describe Microsoft Entra Conditional Access.
- Describe Azure Role Based Access Control (RBAC).
- Describe the concept of Zero Trust.
- Describe the purpose of the defense in depth model.
- Describe the purpose of Microsoft Defender for Cloud.

Continue

Need help? See our troubleshooting guide or provide specific feedback by reporting an issue .

Describe Azure directory services

Completed

- 6 minutes

Microsoft Entra ID is a directory service that enables you to sign in and access both Microsoft cloud applications and cloud applications that you develop. Microsoft Entra ID can also help you maintain your on-premises Active Directory deployment.

For on-premises environments, Active Directory running on Windows Server provides an identity and access management service that's managed by your organization. Microsoft Entra ID is Microsoft's cloud-based identity and access management service. With Microsoft Entra ID, you control the identity accounts, but Microsoft ensures that the service is available globally. If you've worked with Active Directory, Microsoft Entra ID will be familiar to you.

When you secure identities on-premises with Active Directory, Microsoft doesn't monitor sign-in attempts. When you connect Active Directory with Microsoft Entra ID, Microsoft can help protect you by detecting suspicious sign-in attempts at no extra cost. For example, Microsoft Entra ID can detect sign-in attempts from unexpected locations or unknown devices.

Who uses Microsoft Entra ID?

Microsoft Entra ID is for:

- **IT administrators** . Administrators can use Microsoft Entra ID to control access to applications and resources based on their business requirements.
- **App developers** . Developers can use Microsoft Entra ID to provide a standards-based approach for adding functionality to applications that they build, such as adding SSO functionality to an app or enabling an app to work with a user's existing credentials.
- **Users** . Users can manage their identities and take maintenance actions like self-service password reset.
- **Online service subscribers** . Microsoft 365, Microsoft Office 365, Azure, and Microsoft Dynamics CRM Online subscribers are already using Microsoft Entra ID to authenticate into their account.

What does Microsoft Entra ID do?

Microsoft Entra ID provides services such as:

- **Authentication** : This includes verifying identity to access applications and resources. It also includes providing functionality such as self-service password reset, multifactor authentication, a custom list of banned passwords, and smart lockout services.
- **Single sign-on** : Single sign-on (SSO) enables you to remember only one username and one password to access multiple applications. A single identity is tied to a user, which simplifies the security model. As users change roles or leave an organization, access modifications are tied to that identity, which greatly reduces the effort needed to change or disable accounts.
- **Application management** : You can manage your cloud and on-premises apps by using Microsoft Entra ID. Features like Application Proxy, SaaS apps, the My Apps portal, and single sign-on provide a better user experience.
- **Device management** : Along with accounts for individual people, Microsoft Entra ID supports the registration of devices. Registration enables devices to be managed through tools like Microsoft Intune. It also allows for device-based Conditional Access policies to restrict access attempts to only those coming from known devices, regardless of the requesting user account.

Can I connect my on-premises AD with Microsoft Entra ID?

If you had an on-premises environment running Active Directory and a cloud deployment using Microsoft Entra ID, you would need to maintain two identity sets. However, you can connect Active Directory with Microsoft Entra ID, enabling a consistent identity experience between cloud and on-premises.

One method of connecting Microsoft Entra ID with your on-premises AD is using Microsoft Entra Connect. Microsoft Entra Connect synchronizes user identities between on-premises Active Directory and Microsoft Entra ID. Microsoft Entra Connect synchronizes changes between both identity systems, so you can use features like SSO, multifactor authentication, and self-service password reset under both systems.

What is Microsoft Entra Domain Services?

Microsoft Entra Domain Services is a service that provides managed domain services such as domain join, group policy, lightweight directory access protocol (LDAP), and Kerberos/NTLM authentication. Just like Microsoft Entra ID lets you use directory services without having to maintain the infrastructure supporting it, with Microsoft Entra Domain Services, you get the benefit of domain services without the need to deploy, manage, and patch domain controllers (DCs) in the cloud.

A Microsoft Entra Domain Services managed domain lets you run legacy applications in the cloud that can't use modern authentication methods, or where you don't want directory lookups to always go back to an on-premises AD DS environment. You can lift and shift those legacy applications from your on-premises environment into a managed domain, without needing to manage the AD DS environment in the cloud.

Microsoft Entra Domain Services integrates with your existing Microsoft Entra tenant. This integration lets users sign into services and applications connected to the managed domain using their existing credentials. You can also use existing groups and user accounts to secure access to resources. These features provide a smoother lift-and-shift of on-premises resources to Azure.

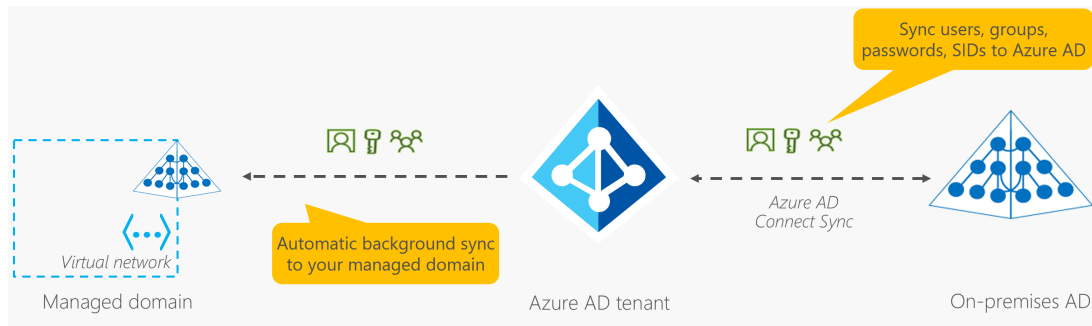
How does Microsoft Entra Domain Services work?

When you create a Microsoft Entra Domain Services managed domain, you define a unique namespace. This namespace is the domain name. Two Windows Server domain controllers are then deployed into your selected Azure region. This deployment of DCs is known as a replica set.

You don't need to manage, configure, or update these DCs. The Azure platform handles the DCs as part of the managed domain, including backups and encryption at rest using Azure Disk Encryption.

Is information synchronized?

A managed domain is configured to perform a one-way synchronization from Microsoft Entra ID to Microsoft Entra Domain Services. You can create resources directly in the managed domain, but they aren't synchronized back to Microsoft Entra ID. In a hybrid environment with an on-premises AD DS environment, Microsoft Entra Connect synchronizes identity information with Microsoft Entra ID, which is then synchronized to the managed domain.



Applications, services, and VMs in Azure that connect to the managed domain can then use common Microsoft Entra Domain Services features such as domain join, group policy, LDAP, and Kerberos/NTLM authentication.

[Continue](#)

Need help? See our troubleshooting guide or provide specific feedback by reporting an issue .

[Describe Azure authentication methods](#)

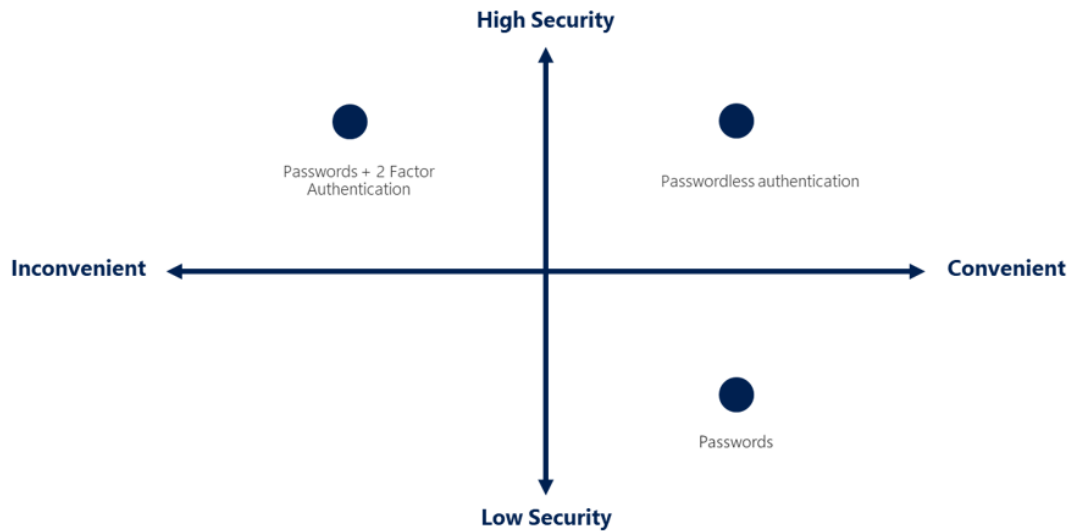
Completed

- 6 minutes

Authentication is the process of establishing the identity of a person, service, or device. It requires the person, service, or device to provide some type of credential to prove who they are. Authentication is like presenting ID when you're traveling. It doesn't confirm that you're ticketed, it just proves that you're who you say you are. Azure supports multiple authentication methods, including standard passwords, single sign-on (SSO), multifactor authentication (MFA), and passwordless.

For the longest time, security and convenience seemed to be at odds with each other. Thankfully, new authentication solutions provide both security and convenience.

The following diagram shows the security level compared to the convenience. Notice Passwordless authentication is high security and high convenience while passwords on their own are low security but high convenience.



What's single sign-on?

Single sign-on (SSO) enables a user to sign in one time and use that credential to access multiple resources and applications from different providers. For SSO to work, the different applications and providers must trust the initial authenticator.

More identities mean more passwords to remember and change. Password policies can vary among applications. As complexity requirements increase, it becomes increasingly difficult for users to remember them. The more passwords a user has to manage, the greater the risk of a credential-related security incident.

Consider the process of managing all those identities. More strain is placed on help desks as they deal with account lockouts and password reset requests. If a user leaves an organization, tracking down all those identities and ensuring they're disabled can be challenging. If an identity is overlooked, this might allow access when it should have been eliminated.

With SSO, you need to remember only one ID and one password. Access across applications is granted to a single identity that's tied to the user, which simplifies the security model. As users change roles or leave an organization, access is tied to a single identity. This change greatly reduces the effort needed to change or disable accounts. Using SSO for accounts makes it easier for users to manage their identities and for IT to manage users.

Important

Single sign-on is only as secure as the initial authenticator because the subsequent connections are all based on the security of the initial authenticator.

What's multifactor authentication?

Multifactor authentication is the process of prompting a user for an extra form (or factor) of identification during the sign-in process. MFA helps protect against a password compromise in situations where the password was compromised but the second factor wasn't.

Think about how you sign into websites, email, or online services. After entering your username and password, have you ever needed to enter a code that was sent to your phone? If so, you've used multifactor authentication to sign in.

Multifactor authentication provides additional security for your identities by requiring two or more elements to fully authenticate. These elements fall into three categories:

- Something the user knows – this might be a challenge question.
- Something the user has – this might be a code that's sent to the user's mobile phone.
- Something the user is – this is typically some sort of biometric property, such as a fingerprint or face scan.

Multifactor authentication increases identity security by limiting the impact of credential exposure (for example, stolen usernames and passwords). With multifactor authentication enabled, an attacker who has a user's password would also need to have possession of their phone or their fingerprint to fully authenticate.

Compare multifactor authentication with single-factor authentication. Under single-factor authentication, an attacker would need only a username and password to authenticate. Multifactor authentication should be enabled wherever possible because it adds enormous benefits to security.

What's Microsoft Entra multifactor authentication?

Microsoft Entra multifactor authentication is a Microsoft service that provides multifactor authentication capabilities. Microsoft Entra multifactor authentication enables users to choose an additional form of authentication during sign-in, such as a phone call or mobile app notification.

What's passwordless authentication?

Features like MFA are a great way to secure your organization, but users often get frustrated with the additional security layer on top of having to remember their passwords. People are more likely to comply when it's easy and convenient to do so. Passwordless authentication methods are more convenient because the password is removed and replaced with something you have, plus something you are, or something you know.

Passwordless authentication needs to be set up on a device before it can work. For example, your computer is something you have. Once it's been registered or enrolled, Azure now knows that it's associated with you. Now that the computer is known, once you provide something you know or are (such as a PIN or fingerprint), you can be authenticated without using a password.

Each organization has different needs when it comes to authentication. Microsoft global Azure and Azure Government offer the following three passwordless authentication options that integrate with Microsoft Entra ID:

- Windows Hello for Business
- Microsoft Authenticator app
- FIDO2 security keys

Windows Hello for Business

Windows Hello for Business is ideal for information workers that have their own designated Windows PC. The biometric and PIN credentials are directly tied to the user's PC, which prevents access from anyone other than the owner. With public key infrastructure (PKI) integration and built-in support for single sign-on (SSO), Windows Hello for Business provides a convenient method for seamlessly accessing corporate resources on-premises and in the cloud.

Microsoft Authenticator App

You can also allow your employee's phone to become a passwordless authentication method. You may already be using the Microsoft Authenticator App as a convenient multifactor authentication option in addition to a password. You can also use the Authenticator App as a passwordless option.

The Authenticator App turns any iOS or Android phone into a strong, passwordless credential. Users can sign-in to any platform or browser by getting a notification to their phone, matching a number displayed on the screen to the one on their phone, and then using their biometric (touch or face) or PIN to confirm. Refer to [Download and install the Microsoft Authenticator app](#) for installation details.

FIDO2 security keys

The FIDO (Fast IDentity Online) Alliance helps to promote open authentication standards and reduce the use of passwords as a form of authentication. FIDO2 is the latest standard that incorporates the web authentication (WebAuthn) standard.

FIDO2 security keys are an unphishable standards-based passwordless authentication method that can come in any form factor. Fast Identity Online (FIDO) is an open standard for passwordless authentication. FIDO allows users and organizations to leverage the standard to sign-in to their resources without a username or password by using an external security key or a platform key built into a device.

Users can register and then select a FIDO2 security key at the sign-in interface as their main means of authentication. These FIDO2 security keys are typically USB devices, but could also use Bluetooth or NFC. With a hardware device that handles the authentication, the security of an account is increased as there's no password that could be exposed or guessed.

[Continue](#)

Need help? See our [troubleshooting guide](#) or provide specific feedback by [reporting an issue](#).

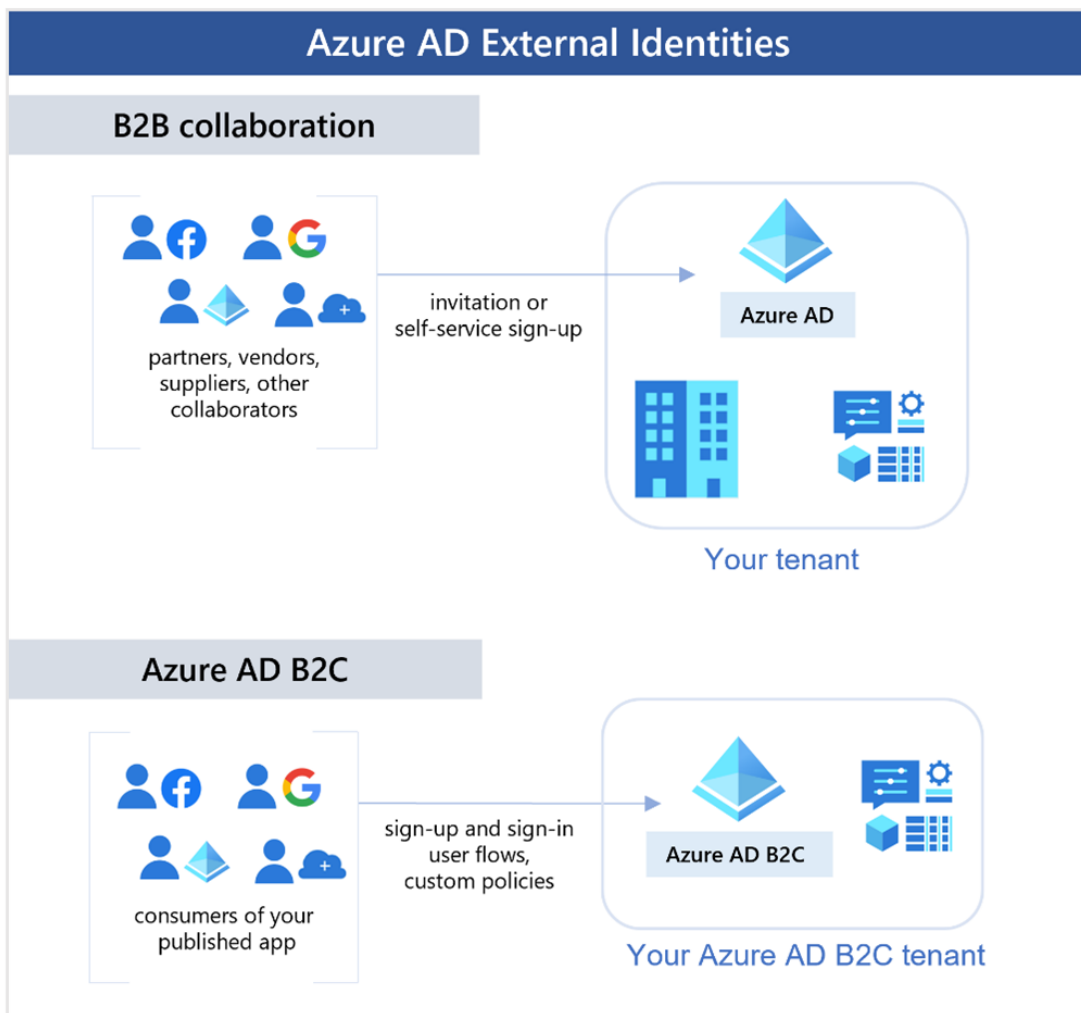
[Describe Azure external identities](#)

Completed

- 3 minutes

An external identity is a person, device, service, etc. that is outside your organization. Microsoft Entra External ID refers to all the ways you can securely interact with users outside of your organization. If you want to collaborate with partners, distributors, suppliers, or vendors, you can share your resources and define how your internal users can access external organizations. If you're a developer creating consumer-facing apps, you can manage your customers' identity experiences.

External identities may sound similar to single sign-on. With External Identities, external users can "bring their own identities." Whether they have a corporate or government-issued digital identity, or an unmanaged social identity like Google or Facebook, they can use their own credentials to sign in. The external user's identity provider manages their identity, and you manage access to your apps with Microsoft Entra ID or Azure AD B2C to keep your resources protected.



The following capabilities make up External Identities:

- **Business to business (B2B) collaboration** - Collaborate with external users by letting them use their preferred identity to sign-in to your Microsoft applications or other enterprise applications (SaaS apps, custom-developed apps, etc.). B2B collaboration users are represented in your directory, typically as guest users.

- **B2B direct connect** - Establish a mutual, two-way trust with another Microsoft Entra organization for seamless collaboration. B2B direct connect currently supports Teams shared channels, enabling external users to access your resources from within their home instances of Teams. B2B direct connect users aren't represented in your directory, but they're visible from within the Teams shared channel and can be monitored in Teams admin center reports.
- **Microsoft Entra business to customer (B2C)** - Publish modern SaaS apps or custom-developed apps (excluding Microsoft apps) to consumers and customers, while using Azure AD B2C for identity and access management.

Depending on how you want to interact with external organizations and the types of resources you need to share, you can use a combination of these capabilities.

With Microsoft Entra ID, you can easily enable collaboration across organizational boundaries by using the Microsoft Entra B2B feature. Guest users from other tenants can be invited by administrators or by other users. This capability also applies to social identities such as Microsoft accounts.

You also can easily ensure that guest users have appropriate access. You can ask the guests themselves or a decision maker to participate in an access review and recertify (or attest) to the guests' access. The reviewers can give their input on each user's need for continued access, based on suggestions from Microsoft Entra ID. When an access review is finished, you can then make changes and remove access for guests who no longer need it.

[Continue](#)

Need help? See our troubleshooting guide or provide specific feedback by reporting an issue .

Describe Azure conditional access

Completed

- 3 minutes

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

Conditional Access helps IT administrators:

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

Conditional Access also provides a more granular multifactor authentication experience for users. For example, a user might not be challenged for second authentication factor if they're at a known location. However, they might be challenged for a second authentication factor if their sign-in signals are unusual or they're at an unexpected location.

During sign-in, Conditional Access collects signals from the user, makes decisions based on those signals, and then enforces that decision by allowing or denying the access request or challenging for a multifactor authentication response.

The following diagram illustrates this flow:



Here, the signal might be the user's location, the user's device, or the application that the user is trying to access.

Based on these signals, the decision might be to allow full access if the user is signing in from their usual location. If the user is signing in from an unusual location or a location that's marked as high risk, then access might be blocked entirely or possibly granted after the user provides a second form of authentication.

Enforcement is the action that carries out the decision. For example, the action is to allow access or require the user to provide a second form of authentication.

When can I use Conditional Access?

Conditional Access is useful when you need to:

- Require multifactor authentication (MFA) to access an application depending on the requester's role, location, or network. For example, you could require MFA for administrators but not regular users or for people connecting from outside your corporate network.
- Require access to services only through approved client applications. For example, you could limit which email applications are able to connect to your email service.
- Require users to access your application only from managed devices. A managed device is a device that meets your standards for security and compliance.
- Block access from untrusted sources, such as access from unknown or unexpected locations.

[Continue](#)

Need help? See our troubleshooting guide or provide specific feedback by reporting an issue .

Describe Azure role-based access control

Completed

- 5 minutes

When you have multiple IT and engineering teams, how can you control what access they have to the resources in your cloud environment? The principle of least privilege says you should only grant access up to the level needed to complete a task. If you only need read access to a storage

blob, then you should only be granted read access to that storage blob. Write access to that blob shouldn't be granted, nor should read access to other storage blobs. It's a good security practice to follow.

However, managing that level of permissions for an entire team would become tedious. Instead of defining the detailed access requirements for each individual, and then updating access requirements when new resources are created or new people join the team, Azure enables you to control access through Azure role-based access control (Azure RBAC).

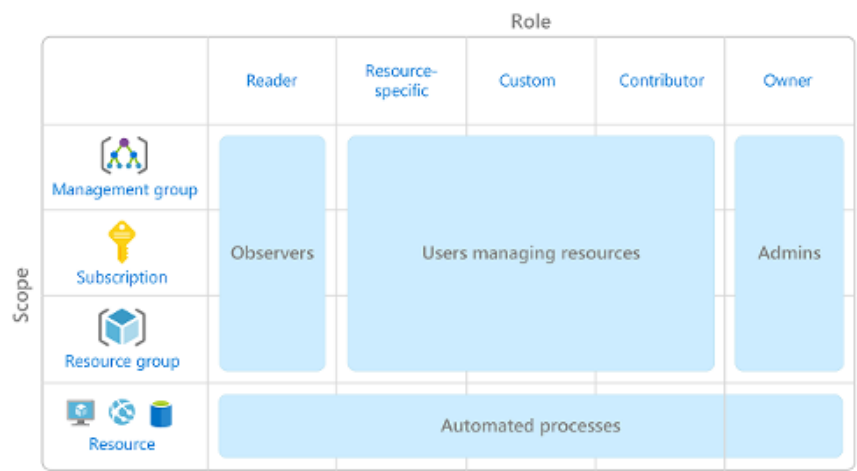
Azure provides built-in roles that describe common access rules for cloud resources. You can also define your own roles. Each role has an associated set of access permissions that relate to that role. When you assign individuals or groups to one or more roles, they receive all the associated access permissions.

So, if you hire a new engineer and add them to the Azure RBAC group for engineers, they automatically get the same access as the other engineers in the same Azure RBAC group. Similarly, if you add additional resources and point Azure RBAC at them, everyone in that Azure RBAC group will now have those permissions on the new resources as well as the existing resources.

How is role-based access control applied to resources?

Role-based access control is applied to a scope, which is a resource or set of resources that this access applies to.

The following diagram shows the relationship between roles and scopes. A management group, subscription, or resource group might be given the role of owner, so they have increased control and authority. An observer, who isn't expected to make any updates, might be given a role of Reader for the same scope, enabling them to review or observe the management group, subscription, or resource group.



Scopes include:

- A management group (a collection of multiple subscriptions).
- A single subscription.
- A resource group.

- A single resource.

Observers, users managing resources, admins, and automated processes illustrate the kinds of users or accounts that would typically be assigned each of the various roles.

Azure RBAC is hierarchical, in that when you grant access at a parent scope, those permissions are inherited by all child scopes. For example:

- When you assign the Owner role to a user at the management group scope, that user can manage everything in all subscriptions within the management group.
- When you assign the Reader role to a group at the subscription scope, the members of that group can view every resource group and resource within the subscription.

How is Azure RBAC enforced?

Azure RBAC is enforced on any action that's initiated against an Azure resource that passes through Azure Resource Manager. Resource Manager is a management service that provides a way to organize and secure your cloud resources.

You typically access Resource Manager from the Azure portal, Azure Cloud Shell, Azure PowerShell, and the Azure CLI. Azure RBAC doesn't enforce access permissions at the application or data level. Application security must be handled by your application.

Azure RBAC uses an allow model. When you're assigned a role, Azure RBAC allows you to perform actions within the scope of that role. If one role assignment grants you read permissions to a resource group and a different role assignment grants you write permissions to the same resource group, you have both read and write permissions on that resource group.

[Continue](#)

Need help? See our troubleshooting guide or provide specific feedback by reporting an issue .

[Describe zero trust model](#)

Completed

- 3 minutes

Zero Trust is a security model that assumes the worst case scenario and protects resources with that expectation. Zero Trust assumes breach at the outset, and then verifies each request as though it originated from an uncontrolled network.

Today, organizations need a new security model that effectively adapts to the complexity of the modern environment; embraces the mobile workforce; and protects people, devices, applications, and data wherever they're located.

To address this new world of computing, Microsoft highly recommends the Zero Trust security model, which is based on these guiding principles:

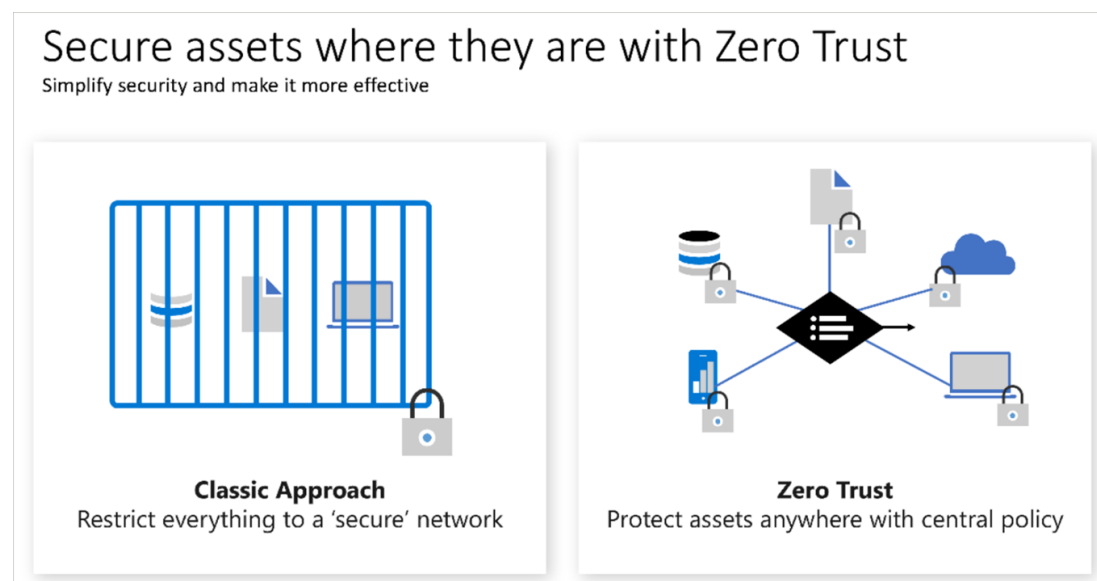
- **Verify explicitly** - Always authenticate and authorize based on all available data points.

- **Use least privilege access** - Limit user access with Just-In-Time and Just-Enough-Access (JIT/JEA), risk-based adaptive policies, and data protection.
- **Assume breach** - Minimize blast radius and segment access. Verify end-to-end encryption. Use analytics to get visibility, drive threat detection, and improve defenses.

Adjusting to Zero Trust

Traditionally, corporate networks were restricted, protected, and generally assumed safe. Only managed computers could join the network, VPN access was tightly controlled, and personal devices were frequently restricted or blocked.

The Zero Trust model flips that scenario. Instead of assuming that a device is safe because it's within the corporate network, it requires everyone to authenticate. Then grants access based on authentication rather than location.



[Continue](#)

Need help? See our troubleshooting guide or provide specific feedback by reporting an issue .

[Describe defense-in-depth](#)

Completed

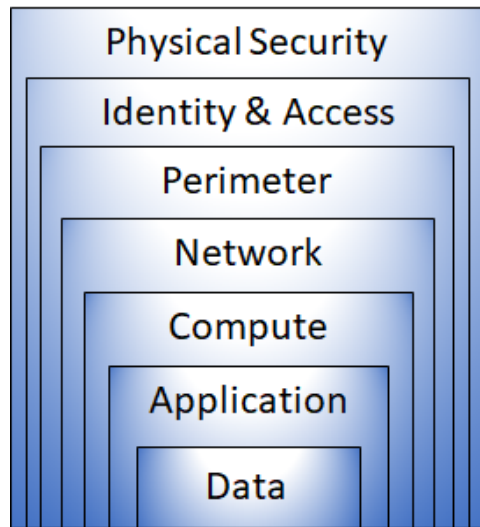
- 4 minutes

The objective of defense-in-depth is to protect information and prevent it from being stolen by those who aren't authorized to access it.

A defense-in-depth strategy uses a series of mechanisms to slow the advance of an attack that aims at acquiring unauthorized access to data.

Layers of defense-in-depth

You can visualize defense-in-depth as a set of layers, with the data to be secured at the center and all the other layers functioning to protect that central data layer.



Each layer provides protection so that if one layer is breached, a subsequent layer is already in place to prevent further exposure. This approach removes reliance on any single layer of protection. It slows down an attack and provides alert information that security teams can act upon, either automatically or manually.

Here's a brief overview of the role of each layer:

- The physical security layer is the first line of defense to protect computing hardware in the datacenter.
- The identity and access layer controls access to infrastructure and change control.
- The perimeter layer uses distributed denial of service (DDoS) protection to filter large-scale attacks before they can cause a denial of service for users.
- The network layer limits communication between resources through segmentation and access controls.
- The compute layer secures access to virtual machines.
- The application layer helps ensure that applications are secure and free of security vulnerabilities.
- The data layer controls access to business and customer data that you need to protect.

These layers provide a guideline for you to help make security configuration decisions in all of the layers of your applications.

Azure provides security tools and features at every level of the defense-in-depth concept. Let's take a closer look at each layer:

Physical security

Physically securing access to buildings and controlling access to computing hardware within the datacenter are the first line of defense.

With physical security, the intent is to provide physical safeguards against access to assets. These safeguards ensure that other layers can't be bypassed, and loss or theft is handled appropriately. Microsoft uses various physical security mechanisms in its cloud datacenters.

Identity and access

The identity and access layer is all about ensuring that identities are secure, that access is granted only to what's needed, and that sign-in events and changes are logged.

At this layer, it's important to:

- Control access to infrastructure and change control.
- Use single sign-on (SSO) and multifactor authentication.
- Audit events and changes.

Perimeter

The network perimeter protects from network-based attacks against your resources. Identifying these attacks, eliminating their impact, and alerting you when they happen are important ways to keep your network secure.

At this layer, it's important to:

- Use DDoS protection to filter large-scale attacks before they can affect the availability of a system for users.
- Use perimeter firewalls to identify and alert on malicious attacks against your network.

Network

At this layer, the focus is on limiting the network connectivity across all your resources to allow only what's required. By limiting this communication, you reduce the risk of an attack spreading to other systems in your network.

At this layer, it's important to:

- Limit communication between resources.
- Deny by default.
- Restrict inbound internet access and limit outbound access where appropriate.
- Implement secure connectivity to on-premises networks.

Compute

Malware, unpatched systems, and improperly secured systems open your environment to attacks. The focus in this layer is on making sure that your compute resources are secure and that you have the proper controls in place to minimize security issues.

At this layer, it's important to:

- Secure access to virtual machines.
- Implement endpoint protection on devices and keep systems patched and current.

Application

Integrating security into the application development lifecycle helps reduce the number of vulnerabilities introduced in code. Every development team should ensure that its applications are secure by default.

At this layer, it's important to:

- Ensure that applications are secure and free of vulnerabilities.
- Store sensitive application secrets in a secure storage medium.
- Make security a design requirement for all application development.

Data

Those who store and control access to data are responsible for ensuring that it's properly secured. Often, regulatory requirements dictate the controls and processes that must be in place to ensure the confidentiality, integrity, and availability of the data.

In almost all cases, attackers are after data:

- Stored in a database.
- Stored on disk inside virtual machines.
- Stored in software as a service (SaaS) applications, such as Office 365.
- Managed through cloud storage.

[Continue](#)

Need help? See our troubleshooting guide or provide specific feedback by reporting an issue .

[Describe Microsoft Defender for Cloud](#)

Completed

- 6 minutes

Defender for Cloud is a monitoring tool for security posture management and threat protection. It monitors your cloud, on-premises, hybrid, and multi-cloud environments to provide guidance and notifications aimed at strengthening your security posture.

Defender for Cloud provides the tools needed to harden your resources, track your security posture, protect against cyber attacks, and streamline security management. Deployment of Defender for Cloud is easy, it's already natively integrated to Azure.

Protection everywhere you're deployed

Because Defender for Cloud is an Azure-native service, many Azure services are monitored and protected without needing any deployment. However, if you also have an on-premises datacenter or are also operating in another cloud environment, monitoring of Azure services may not give you a complete picture of your security situation.

When necessary, Defender for Cloud can automatically deploy a Log Analytics agent to gather security-related data. For Azure machines, deployment is handled directly. For hybrid and multi-cloud environments, Microsoft Defender plans are extended to non Azure machines with the help of Azure Arc. Cloud security posture management (CSPM) features are extended to multi-cloud machines without the need for any agents.

Azure-native protections

Defender for Cloud helps you detect threats across:

- Azure PaaS services – Detect threats targeting Azure services including Azure App Service, Azure SQL, Azure Storage Account, and more data services. You can also perform anomaly detection on your Azure activity logs using the native integration with Microsoft Defender for Cloud Apps (formerly known as Microsoft Cloud App Security).
- Azure data services – Defender for Cloud includes capabilities that help you automatically classify your data in Azure SQL. You can also get assessments for potential vulnerabilities across Azure SQL and Storage services, and recommendations for how to mitigate them.
- Networks – Defender for Cloud helps you limit exposure to brute force attacks. By reducing access to virtual machine ports, using the just-in-time VM access, you can harden your network by preventing unnecessary access. You can set secure access policies on selected ports, for only authorized users, allowed source IP address ranges or IP addresses, and for a limited amount of time.

Defend your hybrid resources

In addition to defending your Azure environment, you can add Defender for Cloud capabilities to your hybrid cloud environment to protect your non-Azure servers. To help you focus on what matters the most, you'll get customized threat intelligence and prioritized alerts according to your specific environment.

To extend protection to on-premises machines, deploy Azure Arc and enable Defender for Cloud's enhanced security features.

Defend resources running on other clouds

Defender for Cloud can also protect resources in other clouds (such as AWS and GCP).

For example, if you've connected an Amazon Web Services (AWS) account to an Azure subscription, you can enable any of these protections:

- Defender for Cloud's CSPM features extend to your AWS resources. This agentless plan assesses your AWS resources according to AWS-specific security recommendations, and includes the results in the secure score. The resources will also be assessed for compliance with built-in standards specific to AWS (AWS CIS, AWS PCI DSS, and AWS Foundational Security Best Practices). Defender for Cloud's asset inventory page is a multi-cloud enabled feature helping you manage your AWS resources alongside your Azure resources.
- Microsoft Defender for Containers extends its container threat detection and advanced defenses to your Amazon EKS Linux clusters.

- Microsoft Defender for Servers brings threat detection and advanced defenses to your Windows and Linux EC2 instances.

Assess, Secure, and Defend

Defender for Cloud fills three vital needs as you manage the security of your resources and workloads in the cloud and on-premises:

- Continuously assess – Know your security posture. Identify and track vulnerabilities.
- Secure – Harden resources and services with Azure Security Benchmark.
- Defend – Detect and resolve threats to resources, workloads, and services.



Continuously assess

Defender for cloud helps you continuously assess your environment. Defender for Cloud includes vulnerability assessment solutions for your virtual machines, container registries, and SQL servers.

Microsoft Defender for servers includes automatic, native integration with Microsoft Defender for Endpoint. With this integration enabled, you'll have access to the vulnerability findings from Microsoft threat and vulnerability management.

Between these assessment tools you'll have regular, detailed vulnerability scans that cover your compute, data, and infrastructure. You can review and respond to the results of these scans all from within Defender for Cloud.

Secure

From authentication methods to access control to the concept of Zero Trust, security in the cloud is an essential basic that must be done right. In order to be secure in the cloud, you have to ensure your workloads are secure. To secure your workloads, you need security policies in place that are tailored to your environment and situation. Because policies in Defender for Cloud are built on top of Azure Policy controls, you're getting the full range and flexibility of a world-class policy solution. In Defender for Cloud, you can set your policies to run on management groups, across subscriptions, and even for a whole tenant.

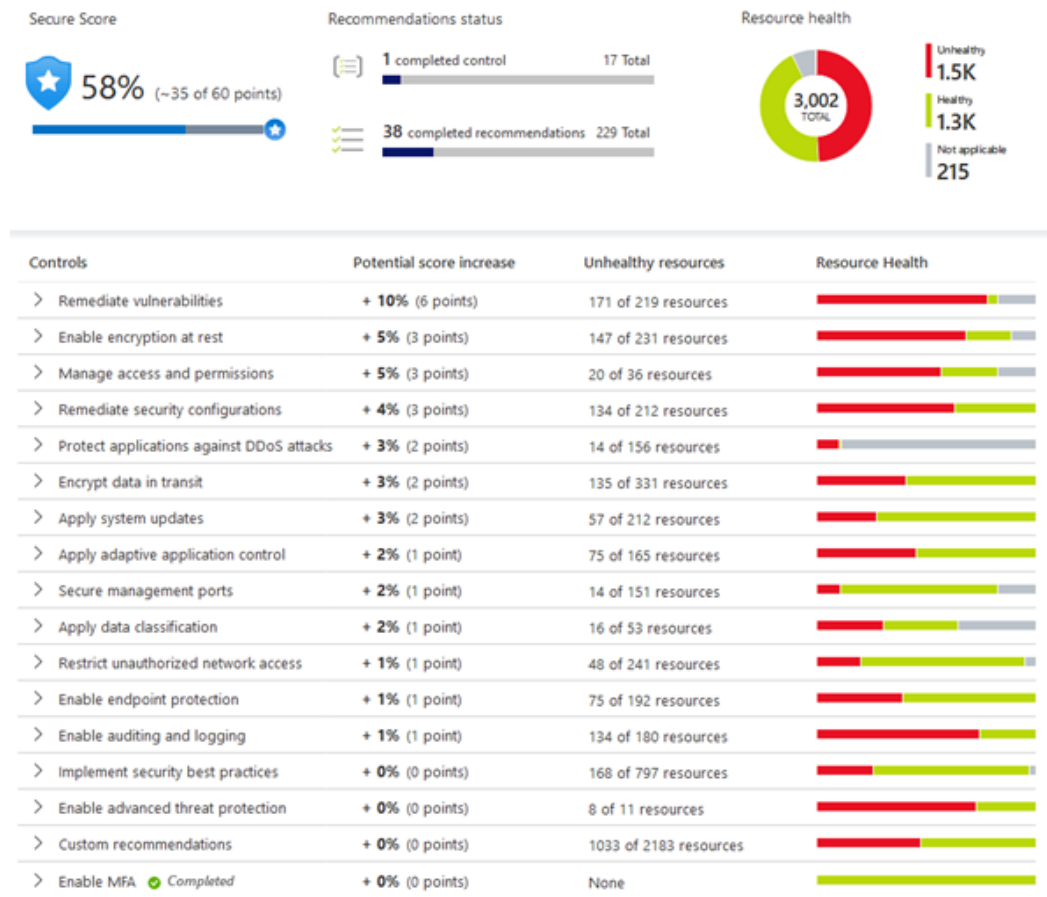
One of the benefits of moving to the cloud is the ability to grow and scale as you need, adding new services and resources as necessary. Defender for Cloud is constantly monitoring for new resources being deployed across your workloads. Defender for Cloud assesses if new resources

are configured according to security best practices. If not, they're flagged and you get a prioritized list of recommendations for what you need to fix. Recommendations help you reduce the attack surface across each of your resources.

The list of recommendations is enabled and supported by the Azure Security Benchmark. This Microsoft-authored, Azure-specific, benchmark provides a set of guidelines for security and compliance best practices based on common compliance frameworks.

In this way, Defender for Cloud enables you not just to set security policies, but to apply secure configuration standards across your resources.

To help you understand how important each recommendation is to your overall security posture, Defender for Cloud groups the recommendations into security controls and adds a secure score value to each control. The secure score gives you an at-a-glance indicator of the health of your security posture, while the controls give you a working list of things to consider to improve your security score and your overall security posture.



Defend

The first two areas were focused on assessing, monitoring, and maintaining your environment. Defender for Cloud also helps you defend your environment by providing security alerts and advanced threat protection features.

Security alerts

When Defender for Cloud detects a threat in any area of your environment, it generates a security alert. Security alerts:

- Describe details of the affected resources
- Suggest remediation steps
- Provide, in some cases, an option to trigger a logic app in response

Whether an alert is generated by Defender for Cloud or received by Defender for Cloud from an integrated security product, you can export it. Defender for Cloud's threat protection includes fusion kill-chain analysis, which automatically correlates alerts in your environment based on cyber kill-chain analysis, to help you better understand the full story of an attack campaign, where it started, and what kind of impact it had on your resources.

Advanced threat protection

Defender for cloud provides advanced threat protection features for many of your deployed resources, including virtual machines, SQL databases, containers, web applications, and your network. Protections include securing the management ports of your VMs with just-in-time access, and adaptive application controls to create allowlists for what apps should and shouldn't run on your machines.

[Continue](#)

Need help? See our troubleshooting guide or provide specific feedback by reporting an issue .

[Knowledge check](#)

Completed

- 4 minutes

Choose the best response for each question. Then select **Check your answers** .

Check your knowledge

1.

Which Microsoft Entra tool can vary the credentials needed to log in based on signals, such as where the user is located?

☐

Conditional Access

☐

Guest access

☐

Passwordless

2.

Which security model assumes the worst-case security scenario, and protects resources accordingly?

☐

Zero trust

☐

Defense-in-depth

☐

Role-based access control

3.

A user is simultaneously assigned multiple roles that use role-based access control. What are their actual permissions? The role permissions are: Role 1 - read || Role 2 - write || Role 3 - read and write.

☐

Read only

☐

Write only

☐

Read and write

Check your answers

You must answer all questions before checking your work.

[Continue](#)

Need help? See our troubleshooting guide or provide specific feedback by reporting an issue .

[Summary](#)

Completed

- 2 minutes

In this module, you learned about Azure identity, access, and security services and tools. You covered authentication methods, including which ones are more secure. You learned about restricting access based on a role to help create a more secure environment. And, you learned about the Defense In Depth and Zero Trust models.

Learning objectives

You should now be able to:

- Describe directory services in Azure, including Microsoft Entra ID and Microsoft Entra Domain Services.
- Describe authentication methods in Azure, including single sign-on (SSO), multifactor authentication (MFA), and passwordless.
- Describe external identities and guest access in Azure.
- Describe Microsoft Entra Conditional Access.
- Describe Azure Role Based Access Control (RBAC).
- Describe the concept of Zero Trust.
- Describe the purpose of the defense in depth model.
- Describe the purpose of Microsoft Defender for Cloud.

Additional resources

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

- [Microsoft Certified: Security, Compliance, and Identity Fundamentals](#) is an entire certification, with associated training, dedicated to helping you better understand and manage Security, Compliance, and identity.

[Continue](#)

Need help? See our troubleshooting guide or provide specific feedback by reporting an issue .

Microsoft Cloud Adoption Framework for Azure

Introduction

Completed

- 1 minute

Azure connects applications to the intelligent edge of connected systems and devices that gather and analyze data. Azure uses AI technology to provide intelligent computing power to these applications, systems, and devices across the world. The connection between the Azure intelligent cloud and the intelligent edge gives organizations the ability to create a new class of connected applications and experiences that drive breakthrough business outcomes. By using the Cloud Adoption Framework for Azure and building the right comprehensive and holistic adoption strategy around business, people, and technology, you can ensure that your organization takes full advantage of Azure to meet your digital transformation goals.

In this module, you will:

- Learn how to use the Cloud Adoption Framework to identify where your organization is in the digital transformation journey.
- Identify triggers and opportunities for cloud adoption.
- Recognize the components needed to develop a digital transformation strategy around your business, people, and technology.

[Continue](#)

Need help? See our troubleshooting guide or provide specific feedback by reporting an issue .

Overview

Completed

- 2 minutes

What is the Microsoft Cloud Adoption Framework for Azure?

The Cloud Adoption Framework for Azure is a collection of documentation, technical guidance, best practices, and tools that aid in aligning business, organizational readiness, and technology strategies. This alignment enables a clear and actionable journey to the cloud that rapidly delivers on the desired business outcomes.

The cloud fundamentally changes how organizations procure and use technology resources. With the cloud, they can provision and consume resources only when needed. While the cloud offers tremendous flexibility in design choices, organizations need a proven and consistent methodology for adopting cloud technologies. The Cloud Adoption Framework meets that need.

It can help guide your decisions throughout cloud adoption to accelerate a specific business objective.

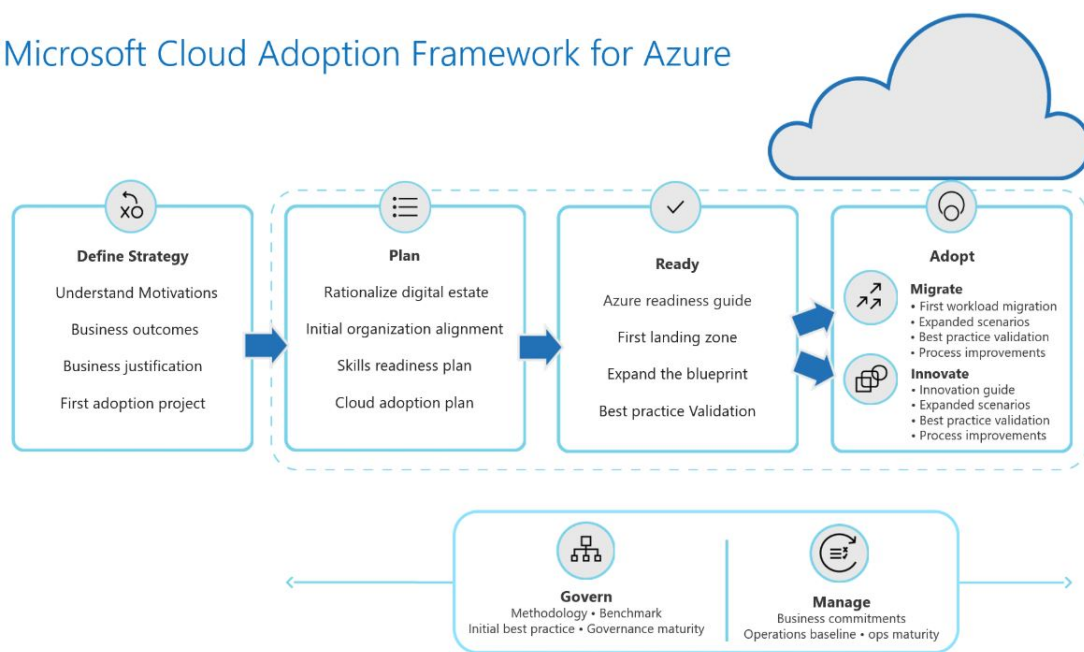
How is it structured?

The Cloud Adoption Framework helps customers undertake a simplified cloud journey in three main stages:

- Plan
- Ready
- Adopt

These three main stages are preceded by a business strategy phase and surrounded by an operations phase that expands through the cloud adoption journey.

Microsoft Cloud Adoption Framework for Azure



The Cloud Adoption Framework contains detailed information to cover an end-to-end cloud adoption journey:

- It begins with setting the business strategy, which should align to actionable technology projects that deliver on the desired business outcomes.
- It then describes how the organization must:
 - Prepare its people with technical readiness.
 - Adjust processes to drive business and technology changes.
 - Enable business outcomes through implementation of the defined technology plan.
- Finally, it covers cloud operations, such as governance, resources, and people and change management.



The cloud offers nearly unlimited potential, but successful adoption requires careful planning and strategy. The adoption strategy depends on where you are in your cloud journey. When you think about your use of the cloud, what is your motivation?

Next, let's define the strategy that might trigger an organization to move to the cloud.

[Continue](#)

Need help? See our troubleshooting guide or provide specific feedback by reporting an issue .

Define strategy

Completed

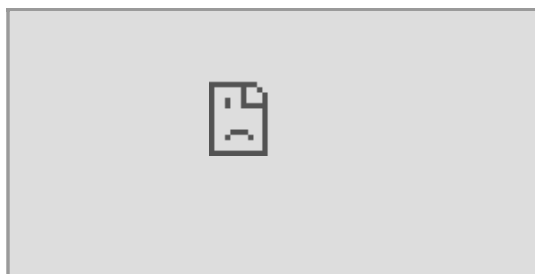
- 10 minutes

Organizations adopt the cloud to help drive business transformation, such as processes and product improvement, market growth, and increased profitability. Let's look at the most common motivation triggers for cloud adoption.

Across organizations of all types, sizes, and industries, the decision to invest in cloud technologies is often tightly connected to a critical business event. The reason for this connection is because the cloud might enable the appropriate solution for the event. Proper cloud technology implementation might turn a reactive response into an innovation opportunity to drive growth for the organization.



Watch this video to learn more.

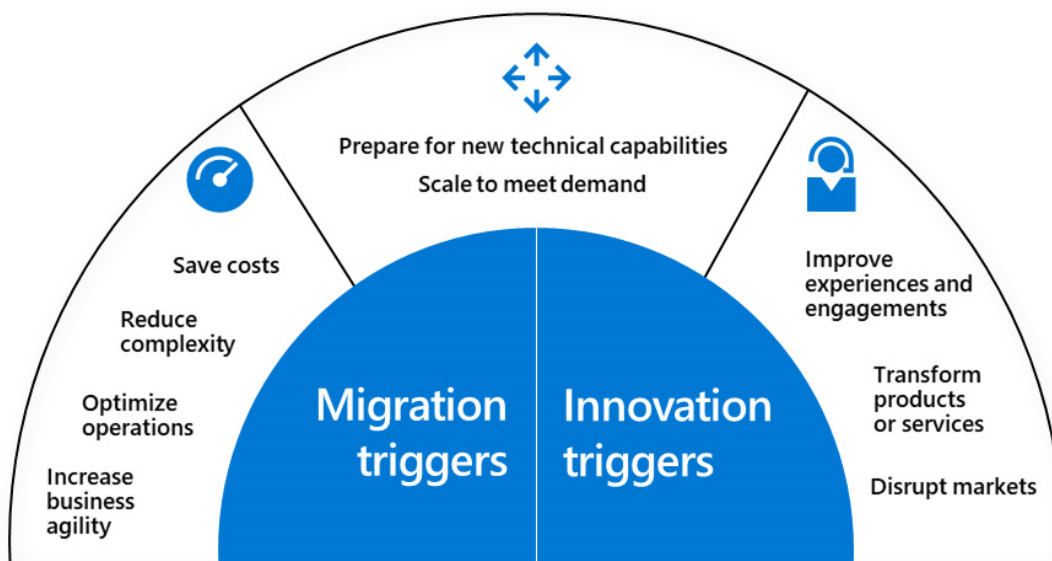


Motivations

Organizations find different triggers to adopt new technologies like Azure. Some triggers drive the organization to migrate current applications. Other triggers require creation of new capabilities, products, and experiences.

Some common migration and innovation triggers include:

- Preparation for new technical capabilities
- Gaining scale to meet market or geographic demands
- Cost savings
- Reduction in vendor or technical complexity
- Optimization of internal operations
- Increased business agility
- Improvements to customer experiences or engagements
- Transformation of products or services
- Disruption of the market from new products or services



There are many reasons or triggers for cloud adoption. Which triggers are most relevant to your business? Where do you see the most opportunity to take advantage of the benefits of cloud technology? Identifying these opportunities will help you develop your cloud adoption plan.

Strategy

When you define your cloud business strategy, you should consider business impact, turnaround time, global reach, performance, and more. Here are key areas you need to focus on:

- **Establish clear business outcomes:** Drive transparency and engagement for your journey across the organization.
- **Define business justification:** Identify business value opportunities to then select the right technology.

Implementing the first application is key to learning and testing with confidence, as your cloud adoption journey starts. Use a two-pronged approach to select it:

- **Business criteria:** Identify an application currently in operation where the owner has a strong motivation to move to the cloud.
- **Technical criteria:** Select an application that has minimum dependencies and can be moved as a small group of assets.



The first application an organization deploys to the cloud is often done so in an experimental environment with no operational or governance capacity. It's important to select an application that doesn't interact with secure data. Carefully consider which application is a good candidate. As you plan subsequent releases and additional applications are deployed to the cloud, you create the first prioritized migration application and the first prioritized release backlog. Over time, you create and continue to shape the optimal environment for future deployments.

Establish clear business outcomes

The most successful cloud adoption journeys start with a business outcome in mind, backed up by financial reasoning and support. A business outcome is a concise, defined, and observable result or change in business performance that's captured by a specific measure. The cloud strategy team consists of business leaders from finance, IT infrastructure, and application groups. The team leads the cloud analysis and planning phase. In this phase, the cloud strategy team is responsible for:

- Reviewing business outcomes and creating the business justification plan for possible use cases for cloud adoption.
- Building or facilitating the cloud rationalization process, selecting the first application, and managing subsequent prioritized backlogs.
- Managing communications with key stakeholders and promoting the cloud adoption journey success and learnings.

Remember that the chief financial officer (CFO) can be a key player in creating and landing a cloud adoption plan and can drive the value of migration and innovation, including creating a financial plan for adoption.

Here are some tools to support you in your financial planning:

- **Azure Total Cost of Ownership (TCO) Calculator:** Use the TCO calculator to estimate the cost savings you can realize by migrating your application workloads to Azure.
- **Azure pricing calculator:** Estimate your expected monthly bill by using the pricing calculator.
- **Microsoft Cost Management + Billing:** Use and manage Azure and other cloud resources through a multiple-cloud cost management solution.

Tip

Links to the TCO calculator, Azure pricing calculator, and Microsoft Cost Management + Billing tools are available in the *Summary and resources* unit at the end of this module.

Define business justification

Developing a clear business justification for cloud adoption with tangible, relevant costs and returns can be a complex process. First, review some common cloud computing business value areas to help justify the cloud adoption journey:

- **Cost:** Eliminates capital expense.
- **Scale:** Ability to scale elastically, delivering the right amount of IT resources
- **Productivity:** Removes the need for many IT management chores
- **Reliability:** Eases the burden of data backup, disaster recovery, and business continuity



Here are the key points from this unit:

- Motivations for cloud adoption include:
 - Migration triggers, such as cost saving and operations optimization.
 - Innovation triggers, such as scaling to meet market or geographical demands.
- The Cloud Adoption Framework for Azure enables an actionable cloud journey that rapidly delivers on the desired business outcomes.
- The key areas to focus on when you develop your cloud business strategy are to:
 - Define your business justification by identifying business value opportunities.
 - Establish clear business outcomes to drive transparency and engagement.
- Microsoft provides tools to support you in your financial planning:
 - Azure total cost of ownership calculator
 - Azure pricing calculator
 - Microsoft Cost Management + Billing
- Your first adoption project should align with your motivations for adoption.

Now that you've learned about how to define your business outcomes and overall strategy for cloud adoption, let's get started and create a plan for this journey.

[Continue](#)

Need help? See our troubleshooting guide or provide specific feedback by reporting an issue .

Plan

Completed

- 5 minutes

How the cloud can advance your business strategy depends on your situation. The cloud delivers fundamental technology benefits that can aid in executing multiple business strategies. Using cloud-based approaches can improve business agility, reduce costs, accelerate time to market, and even allow businesses to quickly expand into new markets.

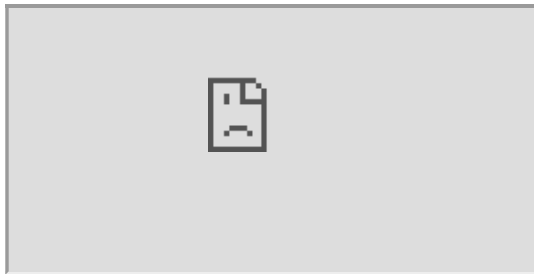
As your organization moves forward in your cloud adoption journey, proper planning is key to your success. Your organization already has technology investments, so you must understand your current state and then develop a prioritization plan for your cloud journey.

In this stage, you focus on two main actions:

- **Rationalize your digital estate:** Understand the organization's current digital estate to maximize return and minimize risks by running a workload assessment.
- **Create your cloud adoption plan:** Develop a plan where prioritized workloads are defined and aligned with business outcomes.



Watch this video to learn more.



Rationalize your digital estate

A digital estate is the collection of IT assets that power business processes and supporting operations. To begin cloud rationalization of the digital estate, inventory all the digital assets the organization owns today. Then, evaluate each asset to determine the best way to migrate or modernize each component to the cloud.

During this process, we recommend that you proceed incrementally, application by application. Don't make decisions too broadly or too early across the entire application portfolio.

There are five options for cloud rationalization, sometimes referred to as the **Five Rs** :

Rationalization option

Expected business outcome



Rehost

Also known as a lift-and-shift migration, a rehost effort moves a current state asset to the chosen cloud provider, with minimal change to overall architecture.

- Reduce capital expense.
- Free up datacenter space.
- Achieve rapid return on investment in the cloud.



Refactor

Refactor also refers to the application development process of refactoring code to allow an application to deliver on new business opportunities.

- Experience faster and shorter updates.
- Benefit from code portability.
- Achieve greater cloud efficiency in the areas of resources, speed, cost.



Rearchitect

When aging applications aren't compatible with the cloud, they might need to be rearchitected to produce cost and operational efficiencies in the cloud.

- Gain application scale and agility.
- Adopt new cloud capabilities more easily.
- Use a mix of technology stacks.



Rebuild/New

Unsupported, misaligned, or out-of-date on-premises applications might be too expensive to carry forward. A new code base with a cloud-native design might be the most appropriate and efficient path.

- Accelerate innovation.
- Build applications faster.
- Reduce operational cost.



Replace

Sometimes the best approach is to replace the current application with a hosted application that meets all functionality required in the cloud.

- Standardize around industry best practices.
- Accelerate adoption of business process-driven approaches.
- Reallocate development investments into applications that create competitive differentiation or advantages.

Create your cloud adoption plan

As you develop a business justification model for your organization's cloud journey, identify business outcomes that can be mapped to specific cloud capabilities and business strategies to reach the desired state of transformation. Documenting all these outcomes and business strategies serves as the foundation for your organization's cloud adoption plan.

Key steps to build this plan are to:

- Review sample business outcomes.

- Identify the leading metrics that best represent progress toward the identified business outcomes.
- Establish a financial model that aligns with the outcomes and learning metrics.

Tip

Links to sample business outcomes, the business outcome template, learning metrics, the financial model, and the digital estate document are available in the *Summary and resources* unit at the end of this module.



Here are the key points from this unit:

- In the plan stage, there are two major actions: rationalizing your digital estate and creating your cloud adoption plan.
- In the Plan phase, there are five options for cloud rationalization: rehost, refactor, rearchitected, rebuild/new, and replace. During this process, we recommend that you proceed incrementally.

Let's talk next about how to prepare your organization, your business processes, and your environment for your cloud adoption journey.

[Continue](#)

Need help? See our troubleshooting guide or provide specific feedback by reporting an issue .

[Ready](#)

Completed

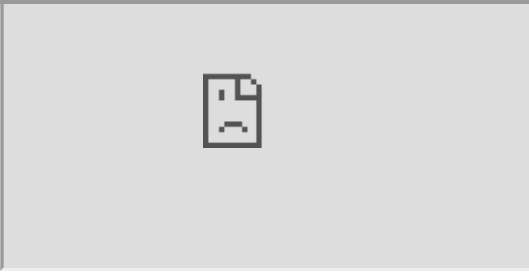
- 8 minutes

We just looked at how a business plan aligned to a digital estate rationalization can ensure you know why you'll benefit from moving to the cloud. Cloud adoption is a strategic change that requires involvement from both business decision makers and end users. Now, let's talk about how to get your organization ready for this journey:

- **Define skills and support readiness:** Create and implement a skills-readiness plan to:
 - Address current gaps.
 - Ensure that IT and business people are ready for the change and the new technologies.
 - Define support needs.
- **Create your landing zone:** Set up a migration target in the cloud to handle prioritized applications.



Watch this video to learn more.



The **Azure readiness guide** introduces features that help you organize resources, control costs, and secure and manage your organization. Links to sample skills-readiness learning paths on Microsoft Learn and Azure Support are available in the *Summary and resources* unit at the end of this module.

Create your landing zone

Before you begin to build and deploy solutions with Azure services, make sure your environment is ready. The term *landing zone* is used to describe an environment that's provisioned and prepared to host workloads in a cloud environment, such as Azure. A fully functioning landing zone is the final deliverable of any iteration of the Cloud Adoption Framework for Azure methodology.



Each landing zone is part of a broader solution for organizing resources across a cloud environment. These resources include management groups, resource groups, and subscriptions. Azure offers many services that help you organize resources, control costs, and secure and manage your organization's Azure subscription. Microsoft Cost Management + Billing also provides a few ways to help you predict, analyze, and manage costs.

Note

For an interactive experience, view the environment-readiness content in the Azure portal. Go to the Azure Quickstart Center in the Azure portal, and select introduction to Azure setup. Then follow the step-by-step instructions.

Tip

Standards-based Azure Blueprints samples are available and ready to use. Visit the list of available samples that are ready to use or modify for your needs, linked in the *Summary and resources* unit at the end of this module.



Here are the key points from this unit:

- Cloud adoption is a strategic change that requires involvement from both business decision makers and end users.
- When you define skills and support readiness, create and implement a skills-readiness plan to address current gaps, ensure that people are ready for the change, and define support needs.
- The process of creating your landing zone sets up a migration target in the cloud to handle prioritized applications.

Next, you'll learn about how to implement your cloud adoption plan based on either a migration or innovation path.

[Continue](#)

Need help? See our troubleshooting guide or provide specific feedback by reporting an issue .

Adopt

Completed

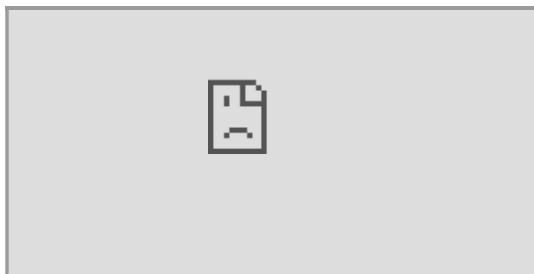
- 7 minutes

At this point, you've established your business justification and defined your business outcomes. You've prepared your organization. Your people and your Azure environment are ready to deploy your prioritized applications. You're ready to adopt cloud technologies following the selected digital estate rationalization path.

As discussed, your organization has unique motivations to adopt the cloud. They all converge into *migration* or *innovation* to the cloud.



Watch this video to learn more.



Cloud migration

Cloud migration is the process of moving existing digital assets to a cloud platform. Existing assets are replicated to the cloud with minimal modifications. After an application or workload becomes operational in the cloud, users are transitioned from the existing solution to the cloud solution.



Cloud migration is one way to effectively balance a cloud portfolio. This is often the fastest and most agile approach in the short term. Conversely, some benefits of the cloud might not be realized without additional future modification. Enterprises and mid-market customers use this approach to accelerate the pace of change, avoid planned capital expenditures, and reduce ongoing operational costs.

The strategy and tools you use to migrate an application to Azure largely depend on your business motivations, technology strategies, and timelines. Your decisions are also based on a deep understanding of the application and the assets to be migrated. These assets include infrastructure, apps, and data. This decision tree serves as high-level guidance to help you select the best tools to use based on migration decisions.

Migration preparation: Establish a rough migration backlog, based largely on the current state and desired outcomes.

- **Business outcomes:** The key business objectives that drive this migration. They're defined in the Plan phase.
- **Digital estate estimate:** A rough estimate of the number and condition of workloads to be migrated. It's defined in the Plan phase.
- **Roles and responsibilities:** A clear definition of the team structure, separation of responsibilities, and access requirements. They're defined in the Ready phase.
- **Change management requirements:** The cadence, processes, and documentation required to review and approve changes. They're defined in the Ready phase.

Cloud innovation

Cloud-native applications and data accelerate development and experimentation cycles. Older applications can take advantage of many of the same cloud-native benefits by modernizing the solution or components of the solution. Modern DevOps and software development lifecycle (SDLC) approaches that use cloud technology shorten the time from idea to product transformation. Combined, these tools invite the customer into the process to create shorter feedback loops and better customer experiences.

Modern approaches to infrastructure deployment, operations, and governance are rapidly bridging the gaps between development and operations. Modernization and innovation in the IT portfolio create tighter alignment with DevOps and accelerate innovations across the digital estate and application portfolio.



Here are the key points from this unit:

- Cloud migration is the process of moving existing digital assets to a cloud platform. Adopt is divided into two different options, migrate and innovate.
- Each cloud migration activity is contained during one of the following processes, as it relates to the migration backlog: assess, migrate, optimize, and secure. Then, you manage

each backlog asset.

- Modernization and innovation in the IT portfolio create tighter alignment with DevOps and accelerate innovations across the digital estate and application portfolio.

You've learned how to plan, get ready, and start to deploy your first applications to the cloud. Now let's talk about governance and management in the cloud.

[Continue](#)

Need help? See our troubleshooting guide or provide specific feedback by reporting an issue .

[Govern and manage](#)

Completed

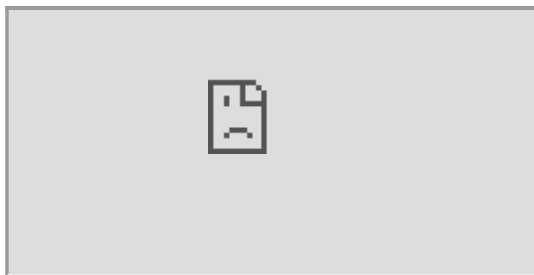
- 6 minutes

The process of adopting the cloud is a journey, not a destination. Along the way, there are clear milestones and tangible business benefits. The final state of cloud adoption is unknown when an organization begins the journey. As your organization moves or deploys new applications to the cloud, this final state starts to form. It's important to consider the following aspects of managing and operating a cloud platform:

- **Define governance solutions for your cloud environment** that meet your organization's business needs, provide agility, and control risks.
- **Manage your cloud environment based on the governance solutions** to allow it to evolve, grow, and adapt to your organization's changing business needs.



Watch this video to learn more.



Cloud governance

Cloud governance creates guardrails that keep the organization on a safe path throughout the journey. The Cloud Adoption Framework for Azure governance model identifies key areas of importance. Each area relates to different types of risks the organization must address as it adopts more cloud services.

Because governance requirements will evolve throughout the cloud adoption journey, a flexible approach to governance is required. IT governance must move quickly and keep pace with business demands to stay relevant during cloud adoption.

Incremental governance relies on a small set of corporate policies, processes, and tools to establish a foundation for adoption and governance. That foundation is called a *minimum viable product (MVP)*. An MVP allows the governance team to quickly incorporate governance into implementations throughout the adoption lifecycle. After this MVP is deployed, additional layers of governance can be quickly incorporated into the environment.

Tip

To determine where you should start to implement your own cloud governance, use the Microsoft assessment tools linked in the *Summary and resources* unit at the end of this module.

Cloud management

The goal of the Manage methodology is to maximize ongoing business returns by creating balance between stability and operational costs. Stable business operations lead to stable revenue streams. Controlled operational costs reduce the overhead to drive more profit from the business processes.

Tip

Links to the scalability, availability, and resiliency resources are available in the *Summary and resources* unit at the end of this module.

Cloud operations creates a maturity model that helps the team fulfill commitments to the business. In the early stages of maturity, customers focus on basic needs such as inventory and visibility into cloud assets and performance. As operations in the cloud mature, the team can use cloud native or hybrid approaches to maintaining operational compliance, which reduces the likelihood of interruptions through configuration and state management. After compliance is achieved, protection and recovery services provide low-impact ways to reduce the duration and effect of business process interruptions. During platform operations, aspects of various platforms (like containers or data platforms) are adjusted and automated to improve performance.



Here are the key points from this unit:

- As your organization moves or deploys new applications to the cloud, it's important to consider these aspects of operating a cloud platform:
 - Define governance solutions for your cloud environment.
 - Manage your cloud environment.
- The Cloud Adoption Framework governance model identifies key areas of importance. Each area relates to different types of risks the organization must address as it adopts more cloud services. The Five Disciplines of Cloud Governance are Cost Management, Security Baseline, Resource Consistency, Identity Baseline, and Deployment Acceleration.

Next, let's see what you've learned about the Cloud Adoption Framework with a knowledge check.

[Continue](#)

Need help? See our troubleshooting guide or provide specific feedback by reporting an issue .

Knowledge check

Completed

- 7 minutes

1.

The Cloud Adoption Framework for Azure helps customers make their journey to the cloud. What are the three main stages of the framework?

☐

Plan, Business Justification, and Implementation.

☐

Migrate, Test, and Optimize.

☐

Plan, Ready, and Adopt.

2.

Motivations for cloud adoption include migration and innovation triggers. Migration triggers include such things as cost saving and operations optimization. Which of the following is an example of an innovation trigger which drives cloud adoption?

☐

Reduction in IT staff for on-premises hardware.

☐

Transform products or services.

☐

Increase business agility.

3.

What are the five disciplines of cloud governance?

☐

Business risk, process, policy and compliance, resource consistency, and deployment acceleration.

☐

Business risk, policy and compliance, security baseline, process, and operations.

☐

Cost management, security baseline, resource consistency, identity baseline, and deployment acceleration.

4.

The common value drivers that business decision makers can use to justify moving their business to the cloud are Cost, Scale, Productivity, and Reliability. What is the specific value of scale in cloud computing?

☐

Scale is the ability to deliver the right amount of IT resources.

☐

Scale eliminates capital expense.

☐

Scale eases the burden of data backup, disaster recovery, and business continuity.

5.

Financial planning for cloud adoption requires organizations to decide whether to expand on-premises capabilities or move certain workloads and functions off-premises to cloud-delivered services. Microsoft has tools that can help. What Microsoft tool is available for a CFO who's trying to estimate the expected monthly bill and track actual account usage?

☐

The Azure Total Cost of Ownership (TCO) Calculator.

☐

The Azure Pricing Calculator.

☐

Microsoft Cost Management.

Check your answers

You must answer all questions before checking your work.

[Continue](#)

Need help? See our troubleshooting guide or provide specific feedback by reporting an issue .

Summary and resources

Completed

- 4 minutes

Moving to the cloud is a complex undertaking. It requires the alignment of senior business leaders on the business value of making the move. They must then create an effective cloud adoption strategy that will be adopted by employees.

The Microsoft Cloud Adoption Framework for Azure can help your business easily identify:

- When to move to the cloud.
- How to create an effective migration strategy.
- Which approach to technology migration and modernization your business should take.

Now that you have reviewed this module, you should be able to:

- Use the Cloud Adoption Framework to identify where you are in the digital transformation journey.
- Identify triggers and opportunities for cloud adoption.
- Recognize the components needed to develop a digital transformation strategy around your business, people, and technology.

Key takeaways

Here are the six key takeaways:



1. The three main components of the Cloud Adoption Framework (plan, ready, and adopt) can be applied to different stages for cloud adopters. They should be revisited often because cloud adoption is an ongoing journey, not a destination.
2. A modernization trigger is an event that initiates the cloud adoption journey for an enterprise. The most common modernization triggers include datacenter contracts expiring, the need to deliver applications and features faster, urgent capacity needs, a software or hardware refresh, the need to address security threats, compliance, enabling new business opportunities, and software end of support.
3. The Plan phase focuses on aligning technology decisions to business priorities, with clear business outcomes and setting the proper cloud rationalization approach.
4. Readyng your people, organization process, and environment for cloud adoption are critical factors in the success of your cloud adoption journey.

5. Adopting the cloud technologies defined in your plan and for which you have readied your organization depends on what you're actually doing. Are you migrating or innovating with a new workload to the cloud?
6. Governing and managing your cloud environment is as critical to your successful cloud adoption as any other stage. As such, it should be considered and executed properly.

Resources

Use these resources to discover more.

Tip

To open a resource link, select and hold (or right-click) and select **Open** in a new tab or window. That way, you can check out the resource and easily return to the module tab to unlock your achievement when you're finished.

Microsoft Cloud Adoption Framework for Azure:

- [Microsoft Cloud Adoption Framework for Azure documentation](#)

Financial planning:

- [Total cost of ownership \(TCO\) calculator](#)
- [Azure pricing calculator](#)
- [Microsoft Cost Management](#)
- [Create a financial model for cloud transformation](#)

Skills readiness paths:

- [Azure fundamentals part 1: describe core Azure concepts](#)
- [Microsoft certified: Azure solutions architect expert](#)
- [Solutions architect: learning path](#)

Cloud migration:

- [Migration in documentation](#)
- [Migration considerations](#)
- [Migration tools decision guide](#)

Cloud governance:

- [Governance in the Cloud Adoption Framework](#)
- [Azure Blueprints samples](#)

Cloud adoption plan:

- Review [sample business outcomes](#).

- Review [approaches to digital estate planning](#).
- Document those findings in the provided [business outcome template](#) to share with internal partners during the transformation journey.
- Identify the [learning metrics](#) that best represent progress toward the identified business outcomes.
- Establish a [financial model](#) that aligns with the outcomes and learning metrics.
- Document and incorporate the [digital estate](#) in the current environment to populate the financial model.

[Continue](#)

Need help? See our troubleshooting guide or provide specific feedback by reporting an issue .

Introduction to the Microsoft Azure Well-Architected Framework

Introduction

Completed

- 2 minutes

Imagine that you're building a new system on the cloud or migrating an existing system to the cloud. How do you instill confidence in your customers that their data is secure? Can your architecture handle a spike in traffic if a media report goes viral? Can your architecture handle the failure of one or more critical components? Are you using resources in the most efficient way?

The Azure Well-Architected Framework helps you to design, build, and continuously improve a secure, reliable, and efficient application. In this module, we introduce you to the framework, along with the pillars and principles that are essential to a great Azure architecture.

The concepts discussed in this module aren't all-inclusive. They represent some of the important considerations when you're building a solution on the cloud. For more details on the Azure Well-Architected Framework, visit the [Azure Architecture Center](#) as you start planning and designing your architecture.

Learning objectives

By the end of this module, you're able to:

- Describe the pillars of the Azure Well-Architected Framework.
- Identify key principles for creating a solid architectural foundation.

Prerequisites

- Experience building or operating solutions by using core infrastructure technology such as data storage, compute, and networking.
- Experience building or operating technology systems to solve business problems.

[Continue](#)

Need help? See our troubleshooting guide or provide specific feedback by reporting an issue .

Azure Well-Architected Framework pillars

Completed

- 10 minutes

The cloud has changed the way organizations solve their business challenges, and how applications and systems are designed. The role of a solution architect isn't limited to delivering business value through the functional requirements of the application. They must also ensure that the solution is designed in ways that are scalable, resilient, efficient, and secure.

Solution architecture is concerned with the planning, design, implementation, and ongoing improvement of a technology system. The architecture of a system must balance and align the business requirements with the technical capabilities that are needed to execute those requirements. The finished architecture is a balance of risk, cost, and capability throughout the system and its components.

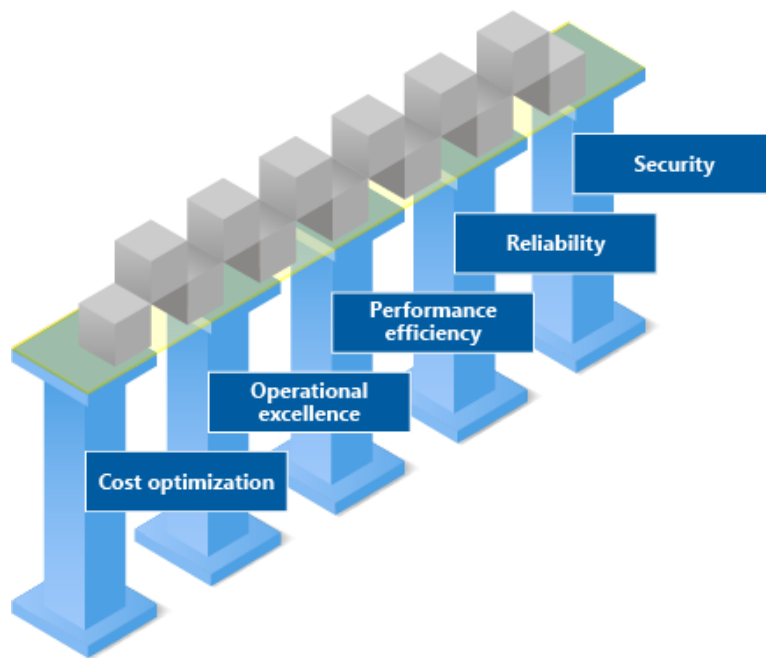
Azure Well-Architected Framework

The Azure Well-Architected Framework is a set of guiding tenets to build high-quality solutions on Azure. There's no one-size-fits-all approach to designing an architecture, but there are some universal concepts that apply regardless of the architecture, technology, or cloud provider.

These concepts aren't all-inclusive, but focusing on them can help you build a reliable, secure, and flexible foundation for your application.

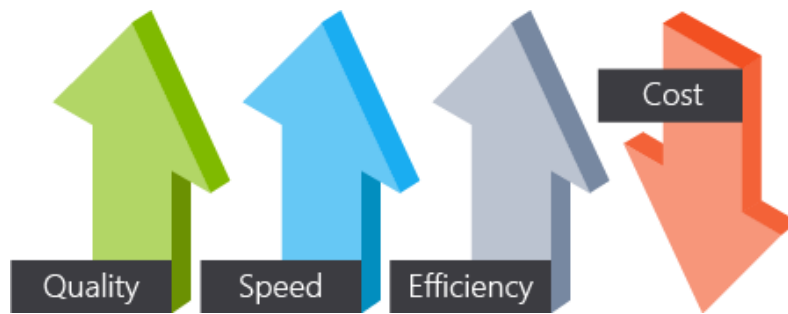
The Azure Well-Architected Framework consists of five pillars:

- Cost optimization
- Operational excellence
- Performance efficiency
- Reliability
- Security



Cost optimization

You want to design your cloud environment so that it's cost-effective for operations and development. Identify inefficiency and waste in cloud spending to ensure you're spending money where you can make the greatest use of it.

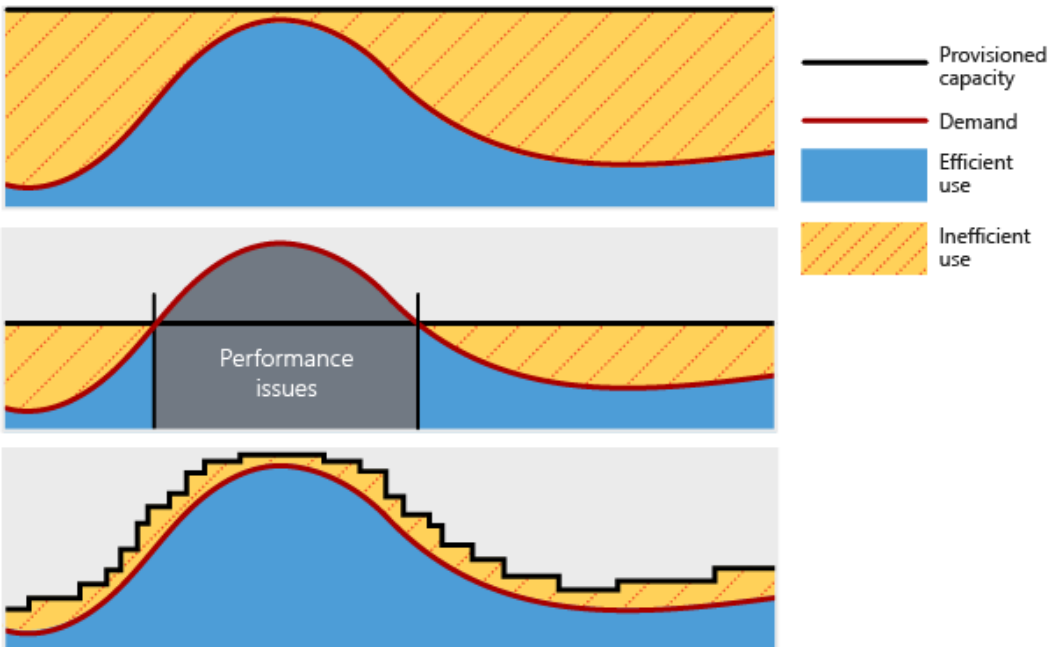


Operational excellence

By taking advantage of modern development practices such as DevOps, you can enable faster development and deployment cycles. You need to have a good monitoring architecture in place so that you can detect failures and problems before they happen or, at a minimum, before your customers notice. Automation is a key aspect of this pillar to remove variance and error while increasing operational agility.

Performance efficiency

For an architecture to perform well and be scalable, it should properly match resource capacity to demand. Traditionally, cloud architectures accomplish this balance by scaling applications dynamically based on activity in the application. Demand for services changes, so it's important for your architecture to be able to adjust to demand. By designing your architecture with performance and scalability in mind, you provide a great experience for your customers while being cost-effective.



Reliability

Every architect's worst fear is having an architecture fail with no way to recover it. A successful cloud environment is designed in a way that anticipates failure at all levels. Part of anticipating failures is designing a system that can recover from a failure within the time that your stakeholders and customers require.



Security

Data is the most valuable piece of your organization's technical footprint. In this pillar, you focus on securing access to your architecture through authentication and protecting your application and data from network vulnerabilities. You should also protect the integrity of your data through tools like encryption.

You must think about security throughout the entire lifecycle of your application, from design and implementation to deployment and operations. The cloud provides protections against various threats, such as network intrusion and DDoS attacks. But you still need to build security into your application, processes, and organizational culture.



General design principles

In addition to each of these pillars, there are some consistent design principles that you should consider throughout your architecture.

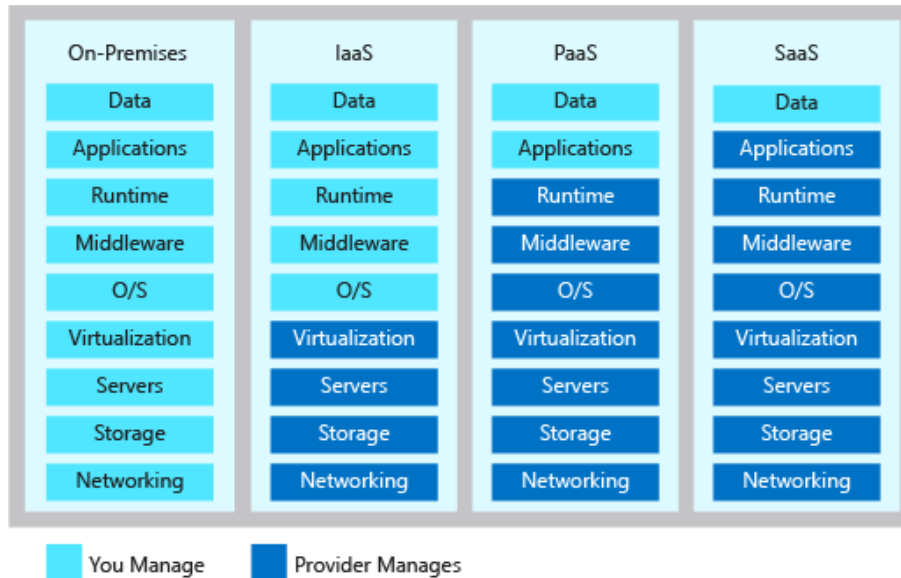
- **Enable architectural evolution** : No architecture is static. Allow for the evolution of your architecture by taking advantage of new services, tools, and technologies when they're available.
- **Use data to make decisions** : Collect data, analyze it, and use it to make decisions surrounding your architecture. From cost data, to performance, to user load, using data can guide you to make the right choices in your environment.
- **Educate and enable** : Cloud technology evolves quickly. Educate your development, operations, and business teams to help them make the right decisions and build solutions to solve business problems. Document and share configurations, decisions, and best practices within your organization.
- **Automate** : Automation of manual activities reduces operational costs, minimizes error introduced by manual steps, and provides consistency between environments.

Shared responsibility

Moving to the cloud introduces a model of shared responsibility. In this model, your cloud provider manages certain aspects of your application, leaving you with the remaining responsibility.

In an on-premises environment, you're responsible for everything. As you move to infrastructure as a service (IaaS), then to platform as a service (PaaS) and software as a service (SaaS), your cloud provider takes on more of this responsibility.

This shared responsibility plays a role in your architectural decisions, because these decisions can have implications on cost, security, and your application's technical and operational capabilities. By shifting these responsibilities to your provider, you can focus on bringing value to your business and move away from activities that aren't a core business function.



Design choices

In an ideal architecture, you'd build the most secure, high-performance, highly available, and efficient environment possible. However, as with everything, there are tradeoffs.

To build an environment with the highest level of all these pillars, there's a cost. That cost might be in money, time to deliver, or operational agility. Every organization has different priorities that affect the design choices that are made in each pillar. As you design your architecture, you need to determine which trade-offs are acceptable and which aren't.

When you're building an Azure architecture, there are many considerations to keep in mind. You want your architecture to be secure, scalable, available, and recoverable. To make that possible, you have to make decisions based on cost, organizational priorities, and risk.

[Continue](#)

Need help? See our [troubleshooting guide](#) or provide specific feedback by [reporting an issue](#).

Cost optimization

Completed

- 10 minutes

Your organization has moved most of its systems to the cloud, but you're now seeing cost increases in areas you didn't expect. After some observation, you realize that you're inefficient across your environment, and you're still doing manual operational work.

In this unit, you learn about cost optimization and look at ways to reduce unnecessary expenses and improve operational efficiencies.

What is cost optimization?

Cost optimization is ensuring that the money your organization spends is being used to maximum effect. Cloud services provide computing as a utility. Technologies in the cloud are provided under a service model, to be consumed on demand. On-demand service offerings drive a fundamental change that directly affects planning, bookkeeping, and organizing.

When an organization decides to own infrastructure, it buys equipment that goes onto the balance sheet as assets. Because a capital investment was made, accountants categorize this transaction as a capital expense (CapEx). Over time, to account for the assets' limited useful lifespan, assets are depreciated or amortized.

Cloud services, on the other hand, are categorized as an operating expense (OpEx) because of their consumption model. Under this scheme, there's no asset to amortize. Instead, OpEx has a direct impact on net profit, taxable income, and the associated expenses on the balance sheet.

When an organization adopts a cloud platform, it must shift away from CapEx-oriented budgeting toward OpEx. This move reflects the shift from owning infrastructure to leasing solutions. Some organizations can derive value just from this new accounting model. For example, a startup company can attract investors by demonstrating a profitable idea at large scale, without needing a large investment up front to purchase infrastructure.

To optimize costs in your organization's architecture, you can use several principles.

Plan and estimate costs

For any cloud project, whether it's the development of a new application or the migration of an entire datacenter, it's important to get an estimate of your costs. This estimate involves identifying any current resources to move or redevelop, understanding business objectives that might affect sizing, and selecting the appropriate services for the project.

With the requirements identified, you can use cost-estimation tools to provide a more concise estimate of the resources that would be required. Transparency is important here, so that all stakeholders can review for accuracy and have visibility into the costs that are associated with the project.

Provision with optimization

Provisioning services that are optimized for cost from the outset can reduce your work effort in the future. For example, you should ensure that you're selecting the appropriate service level for your workload and take advantage of services that let you adjust the service level. You should also use discounts when they're available, such as reserved instances and bring-your-own-license offers.

Where possible, you want to move from IaaS to PaaS services. PaaS services typically cost less than IaaS, and they generally reduce your operational costs.

With PaaS services, you don't have to worry about patching or maintaining VMs, because the cloud provider typically handles those activities. Not all applications can be moved to PaaS, but with the cost savings that PaaS services provide, it's worth considering.

Use monitoring and analytics to gain cost insights

If you're not monitoring your spending, you don't know what you can save. Take advantage of cost-management tools and regularly review billing statements to better understand where money is being spent.

Take time to conduct regular cost reviews across services to understand if the expenditure is appropriate for the resource requirements of the workload. Adjust expenditures as necessary. Identify and track down any cost anomalies that might show up on billing statements or through alerts. If you notice a large spike in cost associated with network traffic, it might uncover both cost savings and potential technical issues.

Maximize efficiency of cloud spend

Efficiency is focused on identifying and eliminating unnecessary expenses within your environment. The cloud is a pay-as-you-go service, and avoidable expenses are typically the result of provisioning more capacity than your demand requires. Operational costs can also contribute to unnecessary or inefficient costs. These inefficient operational costs show up as wasted time and increased error. As you design your architecture, identify and eliminate waste across your environment.

Waste can show up in several ways. Let's look at a few examples:

- A virtual machine that's always 90 percent idle.
- Paying for a license included in a virtual machine when a license is already owned.
- Retaining infrequently accessed data on a storage medium optimized for frequent access.
- Manually repeating the build of a nonproduction environment.

In each of these cases, you're spending more money than you should. Each case presents an opportunity for cost reduction.

As you evaluate your cost, take the opportunity to optimize environments. Capacity demands can and will change over time, and many cloud services can manually or dynamically adjust the provisioned resources to meet the demands. These adjustments can drive the balance between a well-running application and the most cost-effective size.

Optimize your systems at every level. At the network level, ensure that data transfer is efficient and meets the expectations of your customers. Use services to cache data to increase application performance and reduce the transaction load on your data-storage services. Identify and decommission unused resources. Take advantage of lower-cost data-storage tiers to archive infrequently accessed data.

Check your knowledge

1.

Which of the following actions is an example of waste, resulting in an increased resource cost?

☐

Archiving infrequently accessed data to an archive storage tier.

☐

Using a service that automatically adjusts resources that are provisioned to match user load.

☐

Pooling databases to share provisioned capacity.

☐

Running a development environment overnight that is used only during business hours.

2.

Which of the following practices is a good way to reduce costs?

☐

Conducting regular reviews of cloud bills to identify abnormal increases in spend.

☐

Letting all IT teams have access to provision virtual machines of any size.

☐

Provisioning the same capacity in development environments as for production, even though resource requirements are substantially lower in development environments.

☐

Provisioning virtual machines that include licensing costs rather than using a bring-your-own-license image.

3.

Suppose you have recently moved your application to the cloud and your monthly bill seems higher than expected. The utilization level of your VM is high enough that you're hesitant to downsize. What might be a reasonable next step you can take to help you find inefficiencies?

☐

Wait a month and recheck your bill.

☐

Increase the amount of application testing you do before each release.

☐

Add monitoring and instrumentation to your application.

You must answer all questions before checking your work.

[Continue](#)

Need help? See our troubleshooting guide or provide specific feedback by reporting an issue .

Operational excellence

Completed

- 10 minutes

Moving just your resources to the cloud is taking advantage of only a small portion of what the cloud can bring to your organization. Along with the technical capabilities that the cloud delivers, you can improve your operational capabilities as well. From improving developer agility to improving your visibility into the health and performance of your application, you can use the cloud to improve the operational capabilities of your organization.

In this unit, we look at the pillar of operational excellence.

What is operational excellence?

Operational excellence is about ensuring that you have full visibility into how your application is running, and ensuring the best experience for your users. Operational excellence includes making your development and release practices more agile, which allows your business to quickly adjust to changes. By improving operational capabilities, you can have faster development and release cycles, and a better experience for your application's users.

You can use several principles when driving operational excellence through your architecture.

Design, build, and orchestrate with modern practices

Modern architectures should be designed with DevOps and continuous integration in mind. A modern architecture allows you to automate deployments by using infrastructure as code, automate application testing, and build new environments as needed. DevOps is as much cultural as it's technical, but can bring many benefits to organizations that embrace it.

Regardless of the type of project you're managing, you can bring DevOps practices into your organization. Whether your project is an application that uses full continuous integration and continuous deployment (CI/CD) and containers, or a legacy application that you're continuing to service.

Breaking down silos within an organization is a common thread throughout DevOps. So is working collaboratively across every stage in a project, including change management. By creating a culture of sharing, collaboration, and transparency, you can bring operational excellence to your organization.

Use monitoring and analytics to gain operational insights

Throughout your architecture, you want to have a thorough monitoring, logging, and instrumentation system. By creating an effective system for monitoring what's going on in your architecture, you can ensure that you know when something isn't right before your users are affected. With a comprehensive approach to monitoring, you can identify performance issues and cost inefficiencies, correlate events, and gain a greater ability to troubleshoot issues.

Operationally, it's important to have a robust monitoring strategy. Monitoring helps you identify areas of waste, troubleshoot issues, and optimize the performance of your application. A multilayered approach is essential. Gathering data points from components at every layer will help alert you when values are outside acceptable ranges and help you track spending over time.

Use automation to reduce effort and error

You should automate as much of your architecture as possible. The human element is costly, injecting time and error into operational activities. This increased time and error results in increased operational costs. You can use automation to build, deploy, and administer resources. By automating common activities, you can eliminate the delay in waiting for a human to intervene.

Test

You should include testing in your application deployment and your ongoing operations. A good testing strategy helps you identify issues in your application before it's deployed, and ensure that dependent services can properly communicate with your application.

A good testing strategy can also help identify performance issues and potential security vulnerabilities in both preproduction and production deployments. A robust testing plan can uncover issues with infrastructure deployments that can affect the user experience, and testing can help you provide a great experience for your users.

Check your knowledge

1.

Which of the following is a good example of using testing in your environment?

☐

Waiting for users to reach out to you with reports of errors in your application.

☐

Performing functionality tests in the development environment that are different from functionality tests in the production environment.

☐

Omitting infrastructure deployment from test plans.

☐

Performing regular security tests of your application code in development and production environments.

2.

Which of the following examples uses automation to improve operational excellence?

☐

Manually provisioning development environments every day for your development teams.

☐

Logging on Linux VMs after deployment and installing the software packages that are required for the application.

☐

Using a configuration template to deploy infrastructure in each environment.

☐

Manually copying application binaries from your build system to your deployment infrastructure.

Check your answers

You must answer all questions before checking your work.

[Continue](#)

Need help? See our troubleshooting guide or provide specific feedback by reporting an issue .

Performance efficiency

Completed

- 10 minutes

Imagine that a news story is published about one of your organization's recent product announcements. The added publicity from the news story brings a large influx of traffic to your website. Can your website handle this traffic increase? Can your site take on the extra load without becoming slow or unresponsive?

In this unit, we look at some of the basic principles of ensuring outstanding application performance. Especially, the scaling and optimization principles that make up the performance efficiency pillar.

What is performance efficiency?

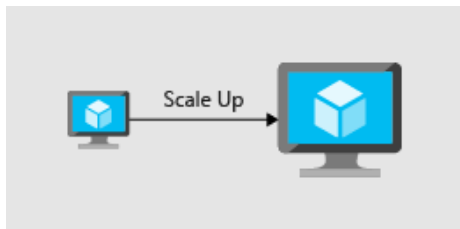
Performance efficiency is matching an application's available resources with the demand that it's receiving. Performance efficiency includes scaling resources, identifying and optimizing potential bottlenecks, and optimizing your application code for peak performance.

Let's look at some patterns and practices that can enhance the scalability and performance of your application.

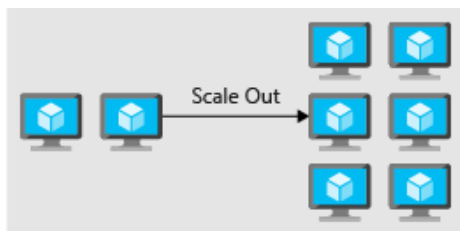
Scale up and scale out

Compute resources can be scaled in two directions:

- Scaling *up* is adding more resources to a single instance. Also known as *vertical scaling*.



- Scaling *out* is adding more instances. Also known as *horizontal scaling*.



Scaling up is concerned with adding more resources, such as CPU or memory, to a single instance. This instance might be a virtual machine or a PaaS service.

The act of adding more capacity to the instance increases the resources that are available to your application, but it does come with a limit. Virtual machines are limited to the capacity of the host on which they run, and hosts themselves have physical limitations. Eventually, when you scale up an instance, you can run into these limits. They restrict your ability to add more resources to the instance.

Scaling out is concerned with adding more instances to a service. They can be virtual machines or PaaS services. Instead of adding more capacity by making a single instance more powerful, we add capacity by increasing the total number of instances.

The advantage of scaling out is that you can conceivably scale out forever if you have more machines to add to the architecture. Scaling out requires some type of load distribution. For example, a load balancer that distributes requests across available servers, or a service-discovery mechanism for identifying active servers to which to send requests.

In both types of scaling, resources can be reduced, which brings cost optimization into the picture.

Autoscaling is the process of dynamically allocating resources to match performance requirements. As the volume of work grows, an application might need more resources to maintain the desired performance levels and satisfy service-level agreements (SLAs). As demand slackens and the added resources are no longer needed, they can be deallocated to minimize costs.

Autoscaling takes advantage of the elasticity of cloud-hosted environments while easing management overhead. It reduces the need for an operator to continually monitor the performance of a system and make decisions about adding or removing resources.

Optimize network performance

When you're optimizing for performance, you look at network and storage performance to ensure that their levels are within acceptable limits. These performance levels can affect the response time of your application. Selecting the right networking and storage technologies for your architecture helps you ensure that you're providing the best experience for your consumers.

Adding a messaging layer between services can have a benefit to performance and scalability. A messaging layer creates a buffer so that requests can continue to flow in without error if the receiving application can't keep up. As the application works through the requests, they're answered in the order in which they were received.

Optimize storage performance

In many large-scale solutions, data is divided into separate partitions that can be managed and accessed separately. The partitioning strategy must be chosen carefully to maximize the benefits while minimizing adverse effects. Partitioning can help improve scalability, reduce contention, and optimize performance.

Use caching in your architecture to help improve performance. Caching is a mechanism to store frequently used data or assets (webpages, images) for faster retrieval. You can use caching at different layers of your application. You can use caching between your application servers and a database in order to decrease data retrieval times.

You can also use caching between your users and your web servers by placing static content closer to users. This type of caching decreases the time it takes to return webpages to the users. It also has a secondary effect of offloading requests from your database or web servers, increasing the performance for other requests.

Identify performance bottlenecks in your application

Distributed applications and services running in the cloud are complex pieces of software that comprise many moving parts. In a production environment, it's important to be able to track the way in which users utilize your system. It's also important to trace resource utilization, and generally monitor the health and performance of your system. You can use this information as a diagnostic aid to detect and correct issues. You can also use this information to help spot potential problems and prevent them from occurring.

Performance optimization includes understanding how the applications themselves are performing. Errors, poorly performing code, and bottlenecks in dependent systems can all be uncovered through an application performance-management tool. Often, these issues might be hidden or obscured for users, developers, and administrators, but they can have an adverse effect on the overall performance of your application.

Look across all layers of your application and identify and remediate performance bottlenecks. These bottlenecks might be poor memory handling in your application, or even the process of adding indexes into your database. It might be an iterative process as you relieve one bottleneck and then uncover another that you were unaware of.

With a thorough approach to performance monitoring, you're able to determine the types of patterns and practices from which your architecture can benefit.

Check your knowledge

1.

Which of the following is an example of scaling up (vertical scaling)?

☐

Updating your application to use a queuing service.

☐

Adding more web servers into a web farm.

☐

Adding another virtual machine into a database cluster.

☐

Updating a virtual machine to a larger size.

2.

Which of the following is an example of scaling out (horizontal scaling)?

☐

Updating a virtual machine to a larger size.

☐

Adding more storage to a virtual machine.

☐

Adding more web servers into a web farm.

☐

Replicating backups to another region

Check your answers

You must answer all questions before checking your work.

[Continue](#)

Need help? See our troubleshooting guide or provide specific feedback by reporting an issue .

Reliability

Completed

- 10 minutes

Imagine that you run a clinical system for a healthcare organization. Clinicians and caregivers have little tolerance for downtime. They need to have access to clinical IT systems around the clock to ensure that they're always providing the highest-quality care.

To meet the around-the-clock demands of clinicians, applications must be able to handle failures with minimal impact to their users. How do they keep their applications operational, both for localized incidents and for large-scale disasters?

In this unit, you learn how to include elements from the reliability pillar in your architecture design.

What is reliability?

In a complex application, any number of things can go wrong at any scale. Individual servers and hard drives can fail. A deployment issue might unintentionally drop all tables in a database. Whole datacenters might become unreachable. A ransomware incident might maliciously encrypt all your data. It's critical that your application stays reliable and can handle both localized and broad-impact incidents.

Designing for reliability includes maintaining uptime through small-scale incidents and temporary conditions like partial network outages. You can ensure that your application handles localized failures by integrating high availability into each component. This application design eliminates single points of failure. Such a design also minimizes the impact of infrastructure maintenance. High-availability designs typically aim to eliminate the impact of incidents quickly and automatically, and to ensure that the system can continue to process requests with little to no effect.

Designing for reliability also focuses on recovery from data loss and from larger-scale disasters. Recovery from these types of incidents often involves active intervention, though automated recovery steps can reduce the time needed to recover. These types of incidents might result in some amount of downtime or permanently lost data. Disaster recovery is as much about careful planning as it is about execution.

Including high availability and recoverability in your architecture design protects your business from financial losses that result from downtime and lost data. They also protect your business from a loss of reputation caused by a loss of trust from your customers.

Architecting for reliability ensures that your application can meet the commitments you make to your customers. You want to ensure that your systems are *available* to end users and can *recover* from any failures.

Build a highly available architecture

For availability, identify the service-level agreement (SLA) to which you're committing. Examine the potential high-availability capabilities of your application relative to your SLA, and identify where you have proper coverage and where you need to make improvements. Your goal is to add redundancy to components of the architecture so that you're less likely to experience an outage.

Examples of high-availability design components include clustering and load balancing:

- Clustering replaces a single VM with a set of coordinated VMs. When one VM fails or becomes unreachable, services can fail over to another one that can service the requests.
- Load balancing spreads requests across many instances of a service, detecting failed instances and preventing requests from being routed to them.

Build an architecture that can recover from failure

For recoverability, you should perform an analysis that examines your possible data loss and major downtime scenarios. Your analysis should include an exploration of recovery strategies and the cost/benefit tradeoff for each. This exercise gives you important insight into your organization's priorities, and helps clarify the role of your application. The results of your analysis should include these duration values for your application:

- **Recovery point objective (RPO)** : The maximum duration of acceptable data loss. RPO is measured in units of time, not volume. Examples are "30 minutes of data," "four hours of data," and so on. RPO is about limiting and recovering from data *loss* , not data *theft* .
- **Recovery time objective (RTO)** : The maximum duration of acceptable downtime, where your specification defines "downtime". For example, if the acceptable downtime duration is eight hours if there's a disaster, then your RTO is eight hours.

With RPO and RTO defined, you can design backup, restore, replication, and recovery capabilities into your architecture to meet these objectives.

Every cloud provider offers a suite of services and features that you can use to improve your application's availability and recoverability. When possible, use existing services and best practices, and try to resist creating your own.

Hard drives can fail, datacenters can become unreachable, and hackers can attack. It's important that you maintain a good reputation with your customers by using availability and recoverability. Availability focuses on maintaining uptime through conditions like network outages, and recoverability focuses on retrieving data after a disaster.

Check your knowledge

1.

Suppose you want to increase the availability of your system to provide a better service-level agreement (SLA) to your customers. Which of the following is a guiding principle you can use?

☐

Reduce your target for maximum duration of acceptable data loss.

☐

Encrypt all data at rest.

☐

Eliminate single point of failure.

2.

Which of the following is affected by your defined recovery point objective (RPO)?

☐

The frequency of database backups.

☐

The number of regions that data is replicated to.

☐

The number of instances in a database cluster.

☐

The type of load-balancing technology used in your application.

You must answer all questions before checking your work.

[Continue](#)

Need help? See our troubleshooting guide or provide specific feedback by reporting an issue .

[Security](#)

Completed

- 10 minutes

Healthcare organizations store personal and potentially sensitive customer data. Financial institutions store account numbers, balances, and transaction histories. Retailers store purchase history, account information, and demographic details of customers. A security incident might expose this sensitive data, which might cause personal embarrassment or financial harm. How do you ensure the integrity of your customer's data and ensure that your systems are secure?

In this unit, you learn about the important elements of the security pillar.

What is security?

Security is ultimately about protecting the data that your organization uses, stores, and transmits. The data that your organization stores or handles is at the heart of your securable assets. This data might be sensitive data about customers, financial information about your organization, or critical line-of-business data that supports your organization. Securing the infrastructure on which the data exists, along with the identities used to access it, is also critically important.

Your data might be subject to more stringent legal and regulatory requirements. These extra requirements depend on where you're located, the type of data you're storing, or the industry in which your application operates.

For instance, in the healthcare industry in the United States, there's a law called the Health Insurance Portability and Accountability Act (HIPAA). In the financial industry, the Payment Card Industry Data Security Standard is concerned with the handling of credit card data. Organizations that store data to which these laws and standards apply, are required to ensure that certain safeguards are in place for the protection of that data. In Europe, the General Data Protection Regulation (GDPR) lays out the rules of how personal data is protected, and defines individuals' rights related to stored data. Some countries/regions require that certain types of data don't leave their borders.

When a security breach occurs, there can be a substantial effect on the finances and reputation of both organizations and customers. A security breach breaks down the trust that customers are willing to instill in your organization, and can affect the organization's long-term health.

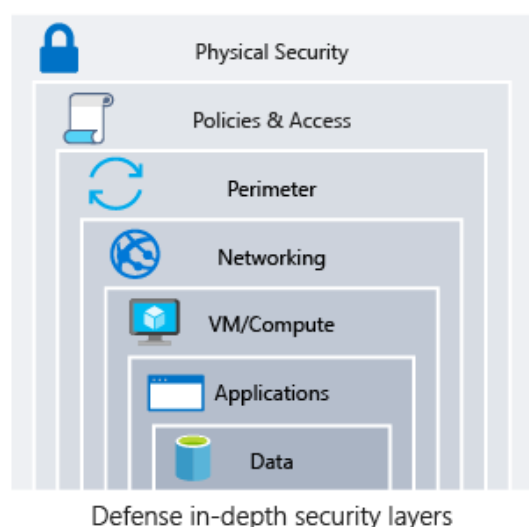
Defense in depth

A multilayered approach to securing your environment increases its security posture. Commonly known as *defense in depth*, we can break down the layers as follows:

- Data
- Applications
- VM/compute
- Networking
- Perimeter
- Policies and access
- Physical security

Each layer focuses on a different area where attacks can happen, and creates a depth of protection if one layer fails or an attacker bypasses it. If you were to focus on just one layer, an attacker would have unfettered access to your environment if they got through this layer.

Addressing security in layers increases the work an attacker must do to gain access to your systems and data. Each layer has different security controls, technologies, and capabilities that apply. When you're identifying the protections to put in place, cost is often of concern. You need to balance cost with business requirements and overall risk to the business.



No single security system, control, or technology fully protects your architecture. Security is more than just technology; it's also about people and processes. Creating an environment that looks holistically at security and makes it a requirement by default helps ensure that your organization is as secure as possible.

Protect from common attacks

At each layer, there are some common attacks that you want to protect against. The following list isn't all-inclusive, but it can give you an idea of how each layer can be attacked and what types of protections you might need.









































- **Data layer** : Exposing an encryption key or using weak encryption can leave your data vulnerable if unauthorized access occurs.
- **Application layer** : Malicious code injection and execution are the hallmarks of application-layer attacks. Common attacks include SQL injection and cross-site scripting (XSS).
- **VM/compute layer** : Malware is a common method of attacking an environment, which involves executing malicious code to compromise a system. After malware is present on a system, further attacks can occur that lead to credential exposure and lateral movement throughout the environment.
- **Networking layer** : Taking advantage of unnecessary open ports to the internet is a common method of attack. Open ports might also include leaving the SSH or RDP protocols



open to virtual machines. When these protocols are open, they can allow brute-force attacks against your systems as attackers attempt to gain access.

- **Perimeter layer** : Denial-of-service (DoS) attacks often happen at this layer. These attacks try to overwhelm network resources, forcing them to go offline or making them incapable of responding to legitimate requests.
- **Policies and access layer** : This layer is where authentication occurs for your application. This layer might include modern authentication protocols such as OpenID Connect, OAuth, or Kerberos-based authentication such as Active Directory. The exposure of credentials is a risk at this layer, and it's important to limit the permissions of identities. You also want to have monitoring in place to look for possible compromised accounts, such as logins coming from unusual places.
- **Physical layer** : Unauthorized access to facilities through methods, such as door drafting and theft of security badges, can happen at this layer.

Shared security responsibility

Revisiting the model of shared responsibility, we can reframe this model in the context of security. Depending on the type of service you select, some security protections are built into the service, while others remain your responsibility. Careful evaluation of the services and technologies you select are necessary, to ensure that you're providing the proper security controls for your architecture.

Responsibility	On-prem	IaaS	PaaS	SaaS
Data governance & rights management				
Client endpoints				
Account & access management				
Identity & directory infrastructure				
Application				
Network controls				
Operating system				
Physical hosts				
Physical network				
Physical datacenter				

 Microsoft
 Customer

Check your knowledge

1.

Which of the following types of data might need to have security protections?

☐

Customer data that contains personal information.

☐

Financial data that supports business operations.

☐

Intellectual property.

☐

All of these types of data might need security protections.

2.

Which of the following examples is an attack you might see at the policies and access layer?

☐

Exposed credentials posted online.

☐

A SYN flood attack.

☐

Following an employee into a datacenter without presenting credentials.

☐

Ransomware that encrypts the disks of a virtual machine.

Check your answers

You must answer all questions before checking your work.

[Continue](#)

Need help? See our troubleshooting guide or provide specific feedback by reporting an issue .

[Summary](#)

Completed

- 2 minutes

Architecture is the foundation of your application's design. Using the Azure Well-Architected Framework will give you the confidence that your app can sustainably meet the needs of your customers both now and in the future.

The architectural priorities and needs of every app are different. The five pillars in the Azure Well-Architected Framework are an excellent guidepost that you can use to make sure that you've given enough attention to every aspect of your application:

- Cost optimization
- Operational excellence
- Performance efficiency
- Reliability
- Security

Focusing on these pillars when designing your architecture ensures that you're laying a solid foundation for your applications in the cloud. With a solid foundation, you're able to drive innovation through your environment, build solutions that your users love, and foster the trust of your customers.

Learn more

For more information on architecting solutions on Azure, visit the [Azure Well-Architected Framework](#) guide in the Azure Architecture Center.

[Continue](#)

Need help? See our troubleshooting guide or provide specific feedback by reporting an issue .