Introduction

- 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.

Next unit: What is Microsoft Azure

What is Microsoft Azure

- 4 minutes

https://learn.microsoft.com/en-us/training/modules/describe-core-architectural-components-of-azure/2-what-microsoft-azure

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

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.

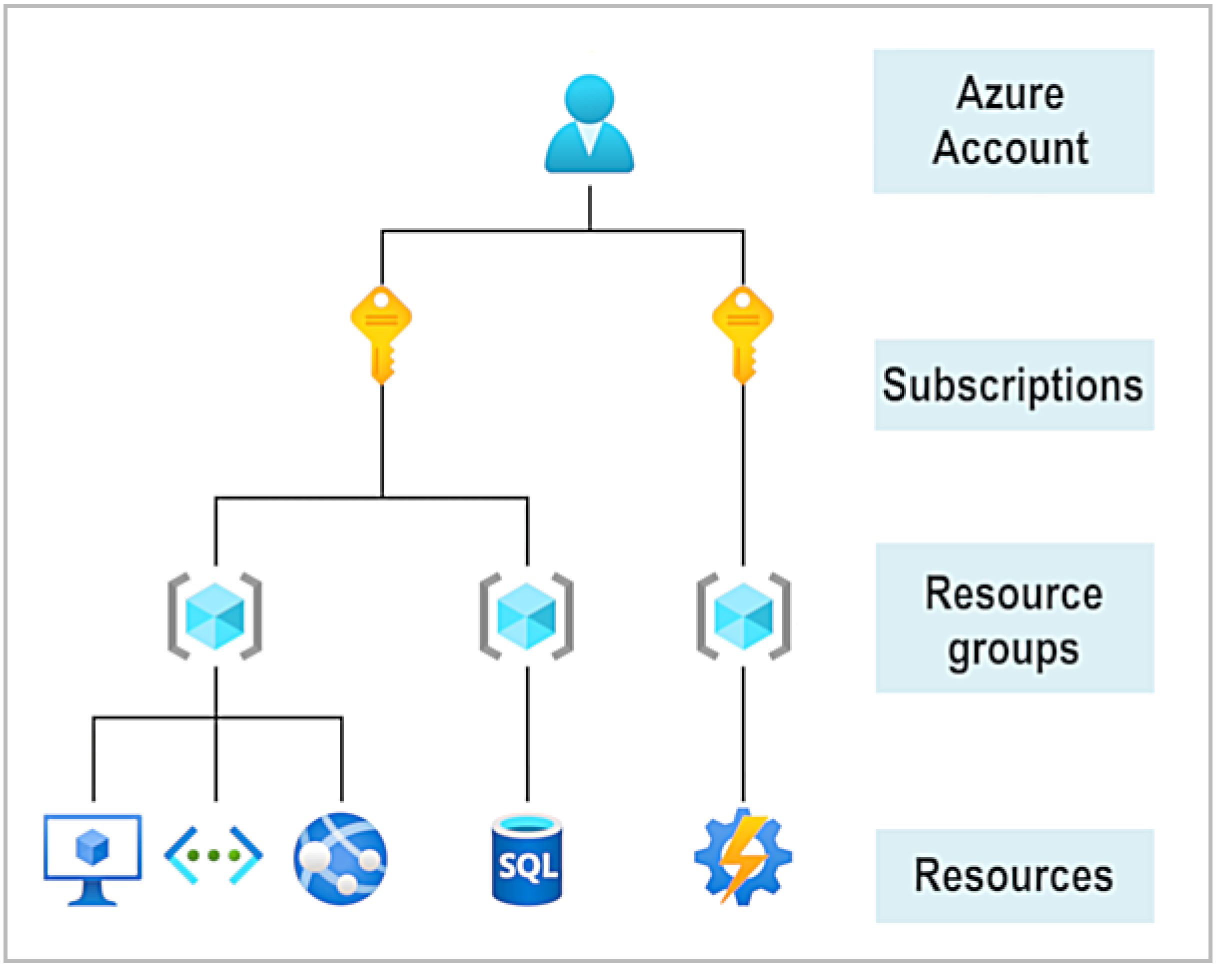
For example, Azure provides artificial intelligence (AI) and machine-learning (ML) services that can naturally communicate with your users through vision, hearing, and speech. It also provides storage solutions that dynamically grow to accommodate massive amounts of data. Azure services enable solutions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

Next unit: Get started with Azure accounts

Get started with Azure accounts

- 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.

https://learn.microsoft.com/en-us/training/modules/describe-core-architectural-components-of-azure/3-get-started-azure-accounts

For more information on how to create an Azure account, see the Create an Azure account learning module.

What is the Azure free account?

The Azure free account includes:

- Free access to popular Azure products for 12 months.
- A credit to 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.

Next unit: Exercise - Explore the Learn sandbox

Exercise - Explore the Learn sandbox

Completed100 XP

- 10 minutes

This module requires a sandbox to complete.

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

Microsoft provides this lab experience and related content for educational purposes. All presented information is owned by Microsoft and intended solely for learning about the covered products and services in this Microsoft Learn module.

Activate sandbox

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

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

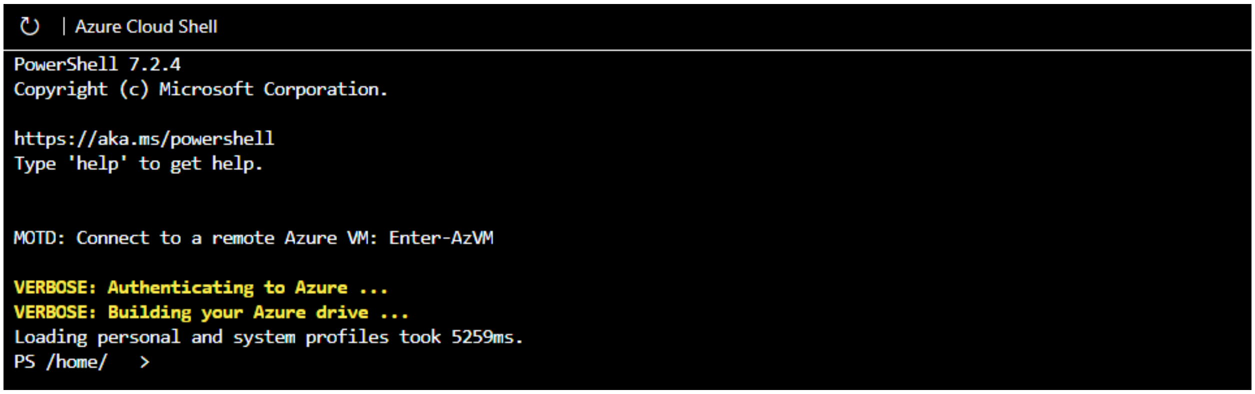
Activate the Learn Sandbox

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

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

Task 1: Use the PowerShell CLI

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



```
PowerShell 7.2.4
Copyright (c) Microsoft Corporation.

https://aka.ms/powershell
Type 'help' to get help.


MOTD: Connect to a remote Azure VM: Enter-AzVM

VERBOSE: Authenticating to Azure ...
VERBOSE: Building your Azure drive ...
Loading personal and system profiles took 5259ms.
PS /home/    >
```

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.

PowerShellCopy

```
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.

PowerShellCopy

```
az version
```

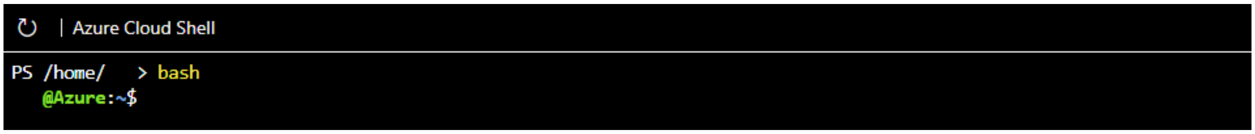
Task 2: Use the BASH CLI

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.

PowerShellCopy

```
bash
```



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

Tip

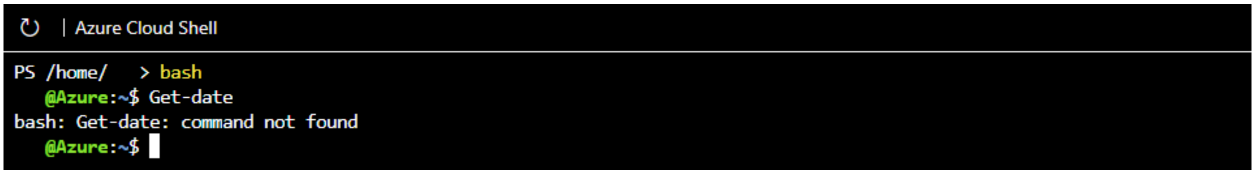
You can tell you're in BASH mode by the username displayed on the command line. It will be your username@azure.

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

Azure CLICopy

```
Get-date
```

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



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

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

Azure CLICopy

```
date
```

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

Azure CLICopy

```
az upgrade
```

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

Task 3: Use Azure CLI interactive mode

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

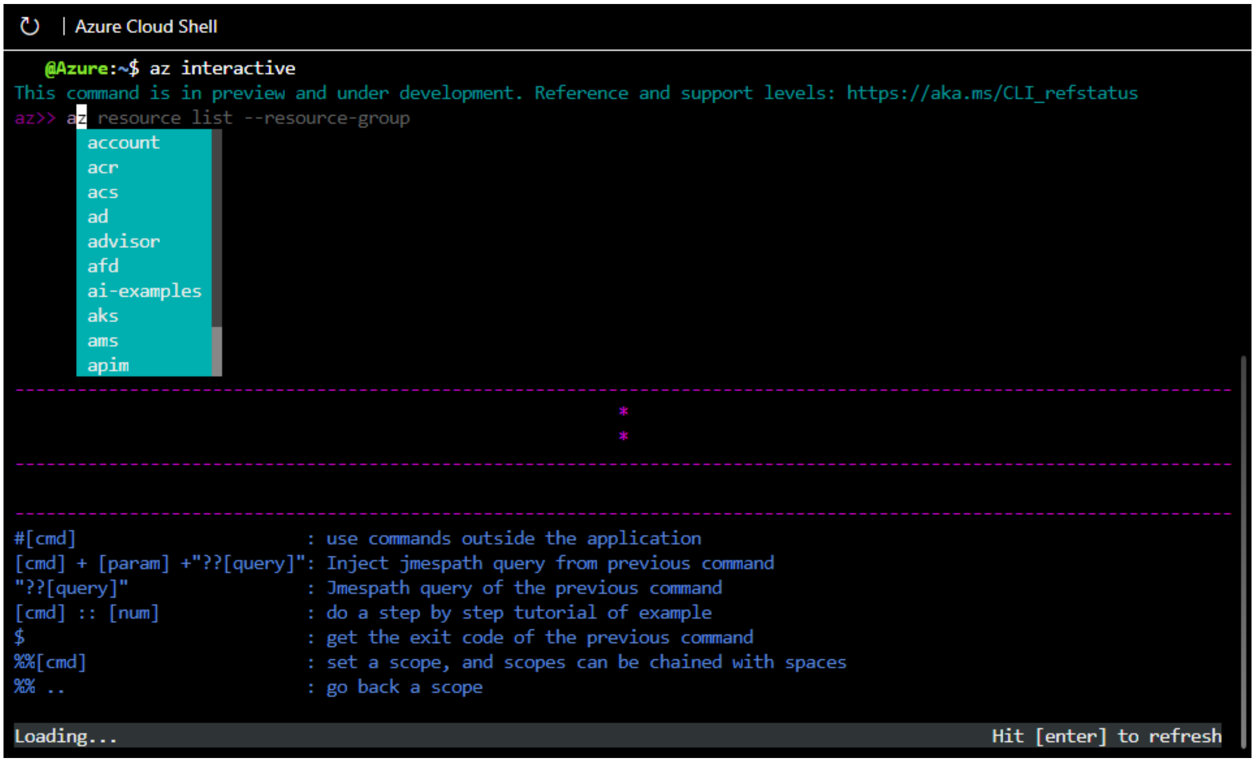
Enter az interactive to enter interactive mode.

Azure CLICopy

```
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:~$ 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

#[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
```

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

Azure CLICopy

```
version
```

Azure CLICopy

```
upgrade
```

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

Azure CLICopy

```
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!

Next unit: Describe Azure physical infrastructure

Describe Azure physical infrastructure

Completed100 XP

- 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.

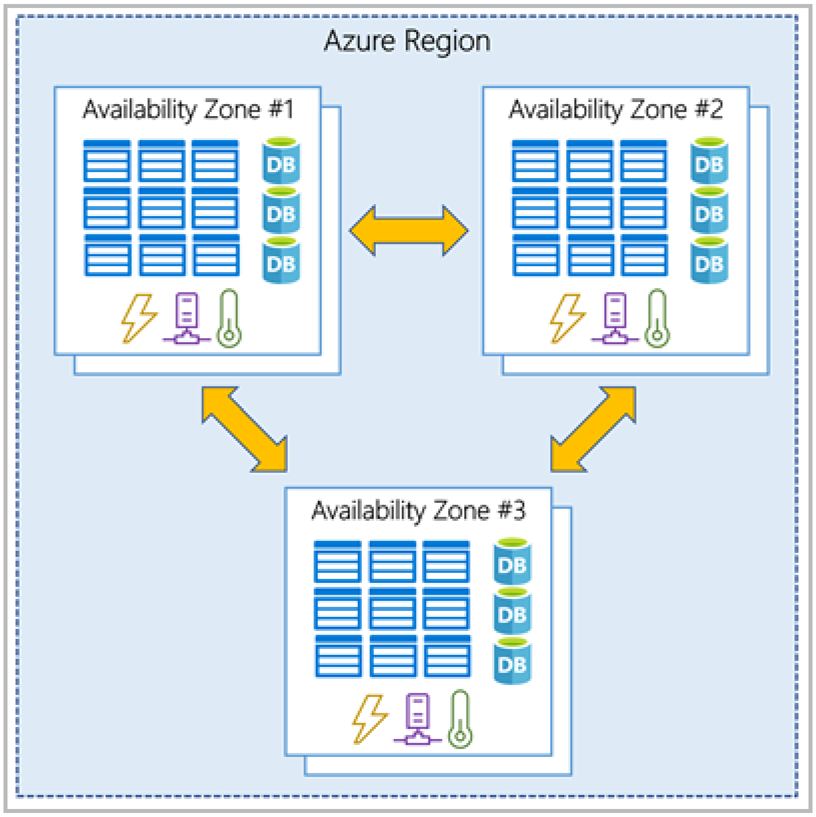
When you deploy a resource in Azure, you'll often need to choose the region where you want your resource deployed.

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 Azure Active Directory, 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.

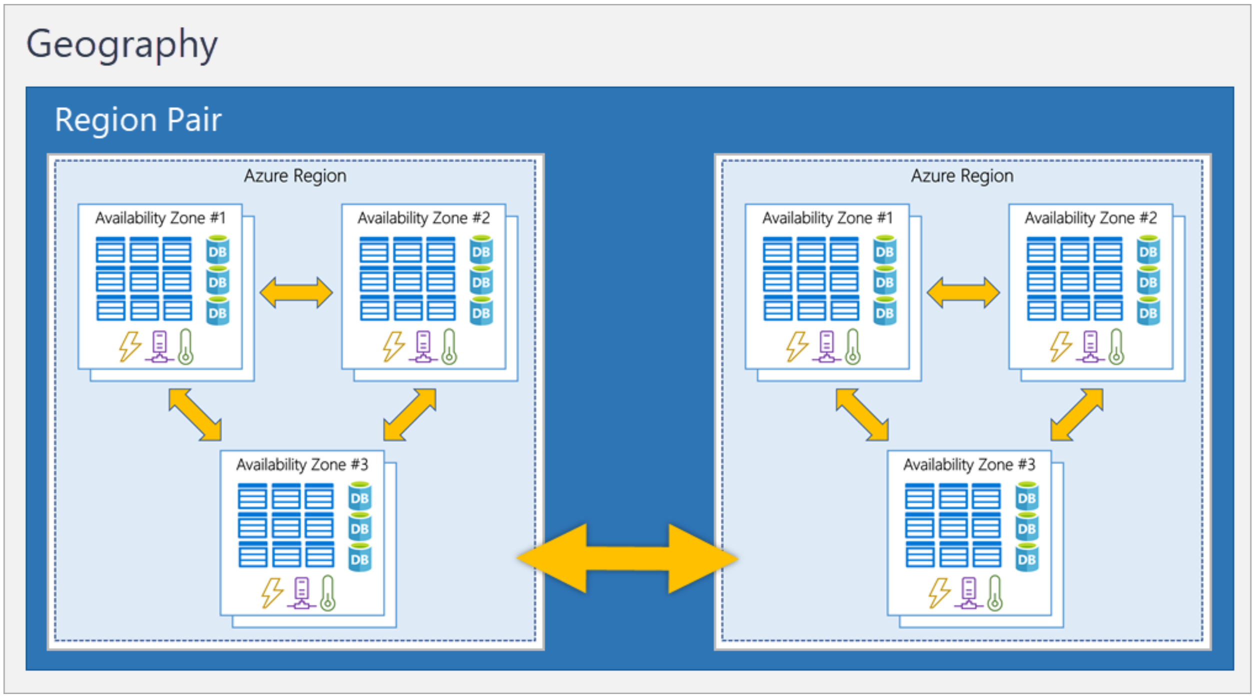
Region pairs

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 directions 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.

Next unit: Describe Azure management infrastructure

Describe Azure management infrastructure

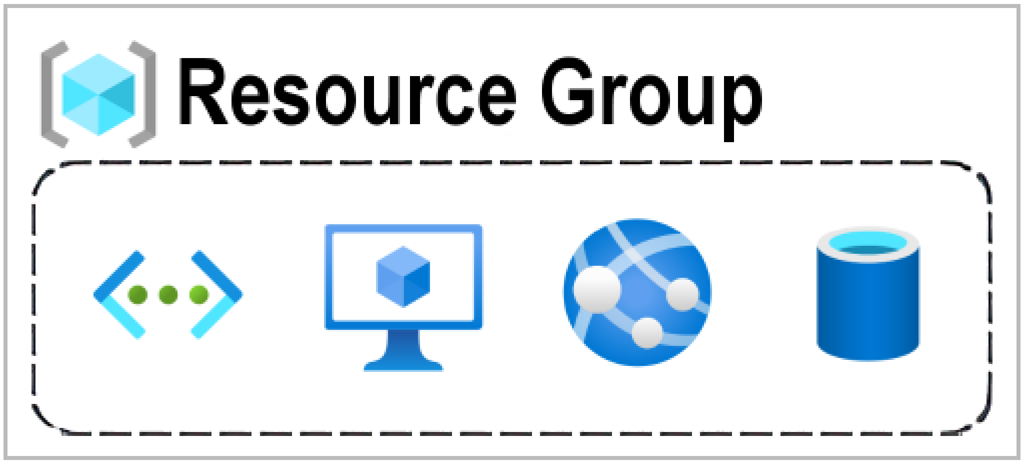
Completed100 XP

- 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.

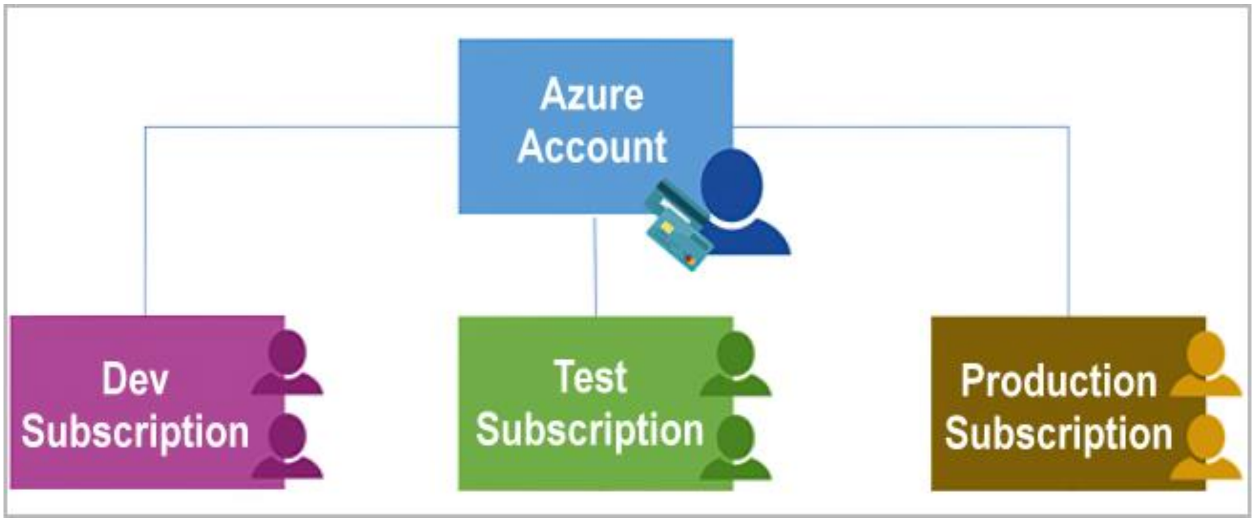
When you’re provisioning resources, it’s good to think about the resource group structure that best suits your needs.

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 Azure Active Directory (Azure AD) or in a directory that Azure AD 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.

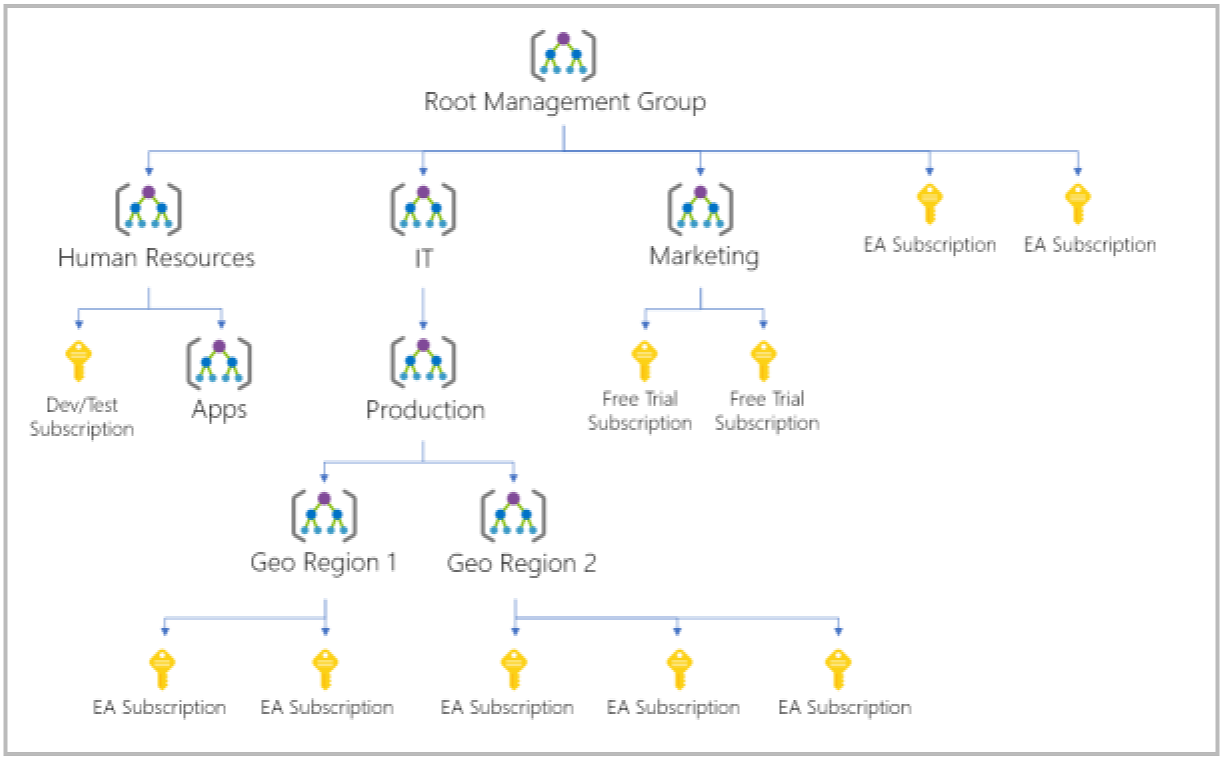
Azure management groups

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.

Next unit: Exercise - Create an Azure resource

Exercise - Create an Azure resource

100 XP

- 10 minutes

This module requires a sandbox to complete.

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

Microsoft provides this lab experience and related content for educational purposes. All presented information is owned by Microsoft and intended solely for learning about the covered products and services in this Microsoft Learn module.

Activate sandbox

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.

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
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.

1. Select Create

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

Task 2: Verify resources created

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

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

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

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

Clean up

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

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

Summary

Completed100 XP

- 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.

Introduction

Completed100 XP

- 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.

Next unit: Describe Azure Virtual Machines

Describe Azure Containers

Completed100 XP

- 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, which is supported by Azure.

Compare virtual machines to containers-0

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

https://learn.microsoft.com/en-us/training/modules/describe-azure-compute-networking-services/5-containers

Azure Container Instances

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

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.

Next unit: Describe Azure Functions

Describe Azure Functions

- 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

https://learn.microsoft.com/en-us/training/modules/describe-azure-compute-networking-services/6-functions

Benefits of Azure Functions

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

Functions scale automatically based on demand, so they may be a good choice when demand is variable.

Azure Functions runs your code when it'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.

Next unit: Describe application hosting options

Describe application hosting options

Completed100 XP

- 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.

Next unit: Describe Azure Virtual Networking

Describe Azure Virtual Networking

Completed100 XP

- 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.

Next unit: Exercise - Configure network access

Exercise - Configure network access

- 10 minutes

This module requires a sandbox to complete.

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

Microsoft provides this lab experience and related content for educational purposes. All presented information is owned by Microsoft and intended solely for learning about the covered products and services in this Microsoft Learn module.

Activate sandbox

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

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:

   Azure CLICopy

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

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

   BashCopy

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

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

   OutputCopy

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

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

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

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

   BashCopy

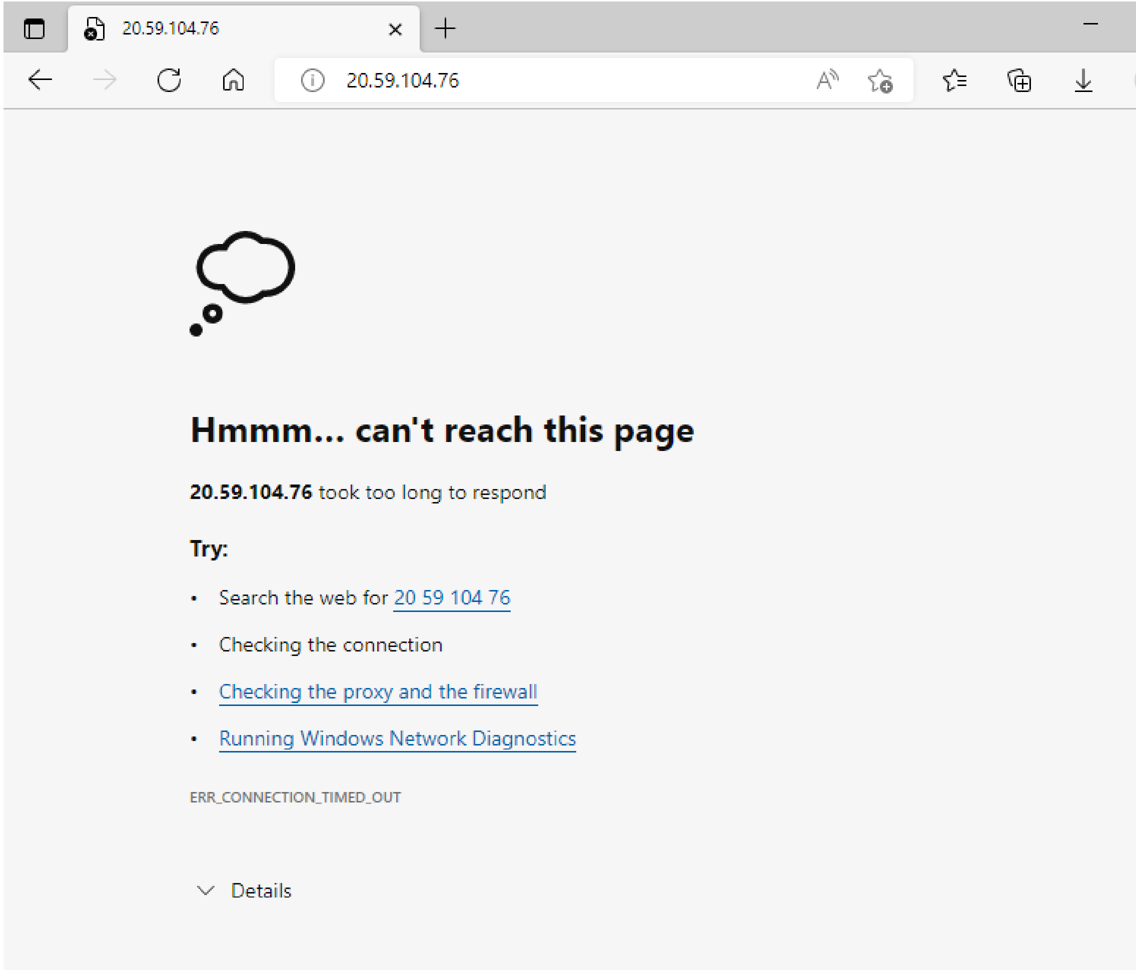
   ```
   echo $IPADDRESS
   ```

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

   b. Copy the IP address that you see to the clipboard.

   c. 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:



Hmmm... can't reach this page

20.59.104.76 took too long to respond

Try:

- Search the web for 20 59 104 76
- Checking the connection
- Checking the proxy and the firewall
- Running Windows Network Diagnostics

ERR_CONNECTION_TIMED_OUT

Details

d. Keep this browser tab open for later.

Task 2: List the current network security group rules

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

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

   Azure CLICopy

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

   You see this:

OutputCopy

```
my-vmNSG
```

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

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

   Azure CLICopy

   ```
   az network nsg rule list \
     --resource-group [sandbox resource group name] \
     --nsg-name my-vmNSG
   ```

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

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

   Azure CLICopy

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

   You see this:

   OutputCopy

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

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

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

Task 3: Create the network security rule

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

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

   Azure CLICopy

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

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

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

   Azure CLICopy

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

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

   OutputCopy

```
Name              Priority    Port    Access
-----------------  ----------  ------  --------
default-allow-ssh  1000        22      Allow
allow-http        100        80      Allow
```

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:

   BashCopy

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

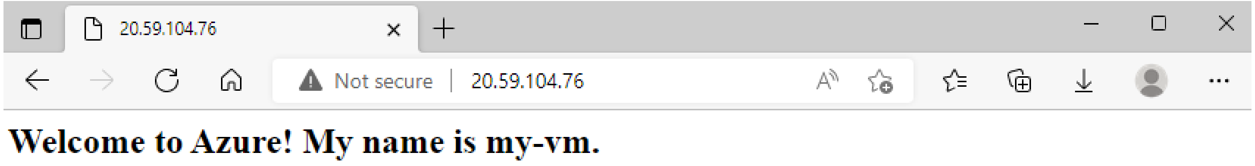
   You see this:

   HTMLCopy

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

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

   You see this:



Welcome to Azure! My name is my-vm.

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.

Next unit: Describe Azure Virtual Private Networks

Describe Azure Virtual Private Networks

Completed100 XP

- 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 you deploy a VPN gateway, you specify the VPN type: either policy-based or route-based. The main difference between these two types of VPNs is how traffic to be encrypted is specified. In Azure, both types of VPN gateways use a pre-shared key as the only method of authentication.

- 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.

Next unit: Describe Azure ExpressRoute

Describe Azure ExpressRoute

- 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.

Next unit: Describe Azure DNS

Describe Azure DNS

Completed100 XP

- 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.

Next unit: Knowledge check

Summary

- 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 associate 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.

Module complete: