

ARM Templates (Azure Resource Manager)

Is the deployment and management service for Azure. It provides a management layer that enables you to create, update, and delete resources in your Azure account.

You can deploy templates to tenants, management groups, subscriptions, or resource groups.

With Resource Manager, you can:

- Manage your infrastructure through declarative templates rather than scripts.
- Deploy, manage, and monitor all the resources for your solution as a group, rather than handling these resources individually.
- Redeploy your solution throughout the development lifecycle and have confidence your resources are deployed in a consistent state.
- Define the dependencies between resources so they're deployed in the correct order
- Apply access control to all services because Azure role-based access control (Azure RBAC) is natively integrated into the management platform.
- Apply tags to resources to logically organize all the resources in your subscription.
- Clarify your organization's billing by viewing costs for a group of resources sharing the same tag.

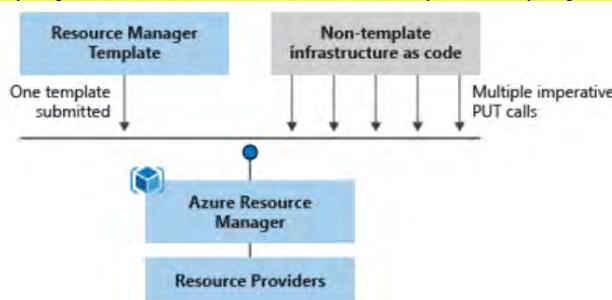
Bicep is a new language for defining your Azure resources. It has a simpler authoring experience than JSON, along with other features that help improve the quality of your infrastructure as code.

The advantages to infrastructure as code are:

- Consistent configurations
- Improved scalability
- Faster deployments
- Better traceability

ARM templates are *idempotent*, which means you can deploy the same template many times and get the same resource types in the same state.

Resource Manager orchestrates the deployment of the resources so they're created in the correct order. When possible, resources will also be created in parallel, so ARM template deployments finish faster than scripted deployments.



It checks the template before starting the deployment to make sure the deployment will succeed. You can also nest templates inside other templates. You can also integrate your ARM

templates into continuous integration and continuous deployment (CI/CD) tools like [Azure Pipelines](#)

Resource groups

There are some important factors to consider when defining your resource group: All the resources in your resource group should share the same lifecycle. You deploy, update, and delete them together. If one resource, such as a server, needs to exist on a different deployment cycle it should be in another resource group.

- Each resource can exist in only one resource group.
- You can add or remove a resource to a resource group at any time.
- You can move a resource from one resource group to another group.
- The resources in a resource group can be located in different regions than the resource group.
- When you create a resource group, you need to provide a location for that resource group.

- A resource group can be used to scope access control for administrative actions. To manage a resource group, you can assign [Azure Policies](#), [Azure roles](#), or [resource locks](#).
- You can [apply tags](#) to a resource group. The resources in the resource group don't inherit those tags.
- A resource can connect to resources in other resource groups. This scenario is common when the two resources are related but don't share the same lifecycle. For example, you can have a web app that connects to a database in a different resource group.
- When you delete a resource group, all resources in the resource group are also deleted.
- You can deploy up to 800 instances of a resource type in each resource group.
- Some resources can exist outside of a resource group. These resources are deployed to the [subscription](#), [management group](#), or [tenant](#). Only specific resource types are supported at these scopes.
- To create a resource group, you can use the [portal](#), [PowerShell](#), [Azure CLI](#), or an [ARM template](#).
- Resource Groups cannot be renamed
- A resource can interact with resources in other resource groups.
-

Exam Tips:

Resources: Vnet, VM, Storage accounts

Resource groups: here you have your resources

Suscriptions: here you have all of your resource groups

Can use REST API endpoints to manage Azure through ARM

Each resource has a resource provider

2. Which of the following situations would be good example of when to use a resource lock?

- A ExpressRoute circuit with connectivity back to the on-premises network.
 - Correct. An ExpressRoute Circuit is a critical resources Resource locks prevent other users in the organization from accidentally deleting or modifying critical resources.**
 - A non-production virtual machine used to test occasional application builds.
 - A storage account used to temporarily store images processed in a development environment.
- X Incorrect. A temporary resource doesn't need to be protected from accidental deletion or modification.**

A service that supplies the resources you can deploy and manage through Resource Manager. Each resource provider offers operations for working with the resources that are deployed. Some common resource providers are Microsoft.Compute, which supplies the virtual machine resource, Microsoft.Storage, which supplies the storage account resource, and Microsoft.Web, which supplies resources related to web apps.

AZURE PORTAL, AZURE CLI AND POWERSHELL

It is the login for the Azure cloud using Azure AD identity and here we can have the azure cli and the cloud shell

Azure Cloud Shell is an interactive, authenticated, browser-accessible shell for managing Azure resources.

Cloudshell:

- Is assigned to one machine per user account.
- Times out after 20 minutes without interactive activity.
- Is temporary and requires a new or existing Azure Files share to be mounted.
- Permissions are set as a regular Linux user in Bash.
- Requires a resource group, storage account, and Azure File share.



Welcome to Azure Cloud Shell

Select Bash or PowerShell. You can change shells any time via the environment selector in the Shell toolbar. The most recently used environment will be the default for your next session.

Bash | PowerShell

Azure CLI and powershell:

- Command Line utility for managing Azure resources for powershell are cmdlets
- Create and manage resources without logging into the Azure Portal
- Create scripts to automate tasks

Inside the bash you can use Azure CLI and inside powershell you can use both powershell and azure cli

COMMANDS:

```
$rg = (Get-AzResourceGroup).ResourceGroupName //Guardan el nombre del resource group
```

```
az group list --query [].name -o tsv
```

```
az vm create --resource-group $rg --name vm-demo-002 --image UbuntuLTS --admin-username  
cloudjorge --generate-ssh-keys //create the vm
```

```
New-AzVM -ResourceGroupName $rg -Name VM-DEMO002 -Image Win2016Datacenter
```

Get-AzResource -ResourceType Microsoft.Compute/virtualMachines // muestra las VMs

Commands in the CLI are structured in *groups* and *subgroups*. Each group represents a service provided by Azure, and the subgroups divide commands for these services into logical groupings. For example, the `storage` group contains subgroups including `account`, `blob`, `share`, and `queue`.

So, how do you find the particular commands you need? One way is to use `az find`. For example, if you want to find commands that might help you manage a storage blob, you can use the find command:

Azure CLI

 Copy

```
az find blob
```

1. Your company is building a video-editing application that will offer online storage for user-generated video content. The videos will be stored in Azure Blobs. An Azure storage account will contain the blobs. It's unlikely the storage account would ever need to be removed and recreated. Which tool is likely to offer the quickest and easiest way to create the storage account?

Azure portal

✓ Correct. The portal is a good choice for one-off operations like creating a long-lived storage account. The portal provides a GUI containing all the storage-account properties and provides tool tips to help select the right options for the organization's needs.

Azure CLI

Azure PowerShell

2. The Azure CLI can be installed on which of the following?

Linux

Windows

Both Linux and Windows

✓ Correct. The CLI is cross-platform and can be installed on Linux, macOS, and Windows. After installation, the CLI commands are the same on every platform.

3. Another Administrator is managing Azure locally using PowerShell. They have launched PowerShell as an Administrator. Which of the following commands should be executed first?

Connect-AzAccount

✓ Correct. So, the first thing to do is to connect to Azure and provide the user credentials.

Get-AzResourceGroup

Get-AzSubscription

Using ARM Templates

This is json code (Declarative)

With this you can:

- use IaC
- Deploy environments quickly
- Repeatable deployments

Components of an ARM template:

- Parameters and variables: used to pass information to the template
- Resources: vms, vnets etc...
- Outputs: Return output from the execution of the template



Link to a template ARM: <https://acloudguru-content-attachment-production.s3-accelerate.amazonaws.com/1642643575999-linuxVM.json>

Link to course to create an ARM: <https://docs.microsoft.com/en-us/learn/modules/create-azure-resource-manager-template-vs-code/>

To deploy in the portal you have to go to the portla and search template, there you paste your ARM template and wait for it to be saved and then you open it and click deploy. You can also do it by console with:

```
Azure PowerShell

$templateFile="azuredeploy.json"
$today=Get-Date -Format "MM-dd-yyyy"
$deploymentName="blanktemplate-"+$today
New-AzResourceGroupDeployment
    -Name $deploymentName
    -TemplateFile $templateFile
```

```
JSON Copy

{
  "$schema": "https://schema.management.azure.com/schemas/2019-04-01/deploymentTemplate.json#",
  "contentVersion": "1.0.0.1",
  "apiProfile": "",
  "parameters": {},
  "variables": {},
  "functions": [],
  "resources": [
    {
      "type": "Microsoft.Storage/storageAccounts",
      "apiVersion": "2019-06-01",
      "name": "learntemplatestorage123",
      "location": "westus",
      "sku": {
        "name": "Standard_LRS"
      },
      "kind": "StorageV2",
      "properties": {
        "supportsHttpsTrafficOnly": true
      }
    }
  ],
  "outputs": {}
}
```

JSON

Copiar

```
"parameters": {  
    "adminUsername": {  
        "type": "string",  
        "metadata": {  
            "description": "Username for the Virtual Machine."  
        }  
    },  
    "adminPassword": {  
        "type": "securestring",  
        "metadata": {  
            "description": "Password for the Virtual Machine."  
        }  
    }  
}
```

Las plantillas de inicio rápido de Azure son plantillas de Azure Resource Manager que proporciona la comunidad de Azure.

3. ¿Qué ocurre si la misma plantilla se ejecuta una segunda vez?

- Azure Resource Manager implementará los recursos nuevos como copias de los que ya se hayan implementado.
- Azure Resource Manager no realizará ningún cambio en los recursos implementados.

✓ Correcto. Si el recurso ya existe y no se detecta ningún cambio en las propiedades, no se realizará ninguna acción. Si el recurso ya existe y se produce un cambio en alguna propiedad, el recurso se actualiza. Si el recurso no existe, se creará.
- Azure Resource Manager eliminará los recursos que ya se hayan implementado y los volverá a implementar.

✗ Incorrecto. Si el recurso ya existe y no se detecta ningún cambio en las propiedades, no se realizará ninguna acción. Si el recurso ya existe y se produce un cambio en alguna propiedad, el recurso se actualiza. Si el recurso no existe, se creará.

Managing Subscriptions and Regions

A region is a geographical area on the planet containing at least one, but potentially multiple datacenters. The datacenters are in close proximity and networked together with a low-latency network.

Azure is generally available in more than 60 regions in 140 countries

Most Azure regions are paired with another region within the same geography to make a *regional pair* (or *paired regions*). Regional pairs help to support always-on availability of Azure resources used by your infrastructure.

Characteristic	Description
Physical isolation	Azure prefers at least 300 miles of separation between datacenters in a regional pair. This principle isn't practical or possible in all geographies. Physical datacenter separation reduces the likelihood of natural disasters, civil unrest, power outages, or physical network outages affecting both regions at once.
Platform-provided replication	Some services like Geo-Redundant Storage provide automatic replication to the paired region.
Region recovery order	During a broad outage, recovery of one region is prioritized out of every pair. Applications that are deployed across paired regions are guaranteed to have one of the regions recovered with priority.
Sequential updates	Planned Azure system updates are rolled out to paired regions sequentially (not at the same time). Rolling updates minimizes downtime, reduces bugs, and logical failures in the rare event of a bad update.
Data residency	Regions reside within the same geography as their enabled set (except for the Brazil South and Singapore regions).

Things to consider when using regions and regional pairs

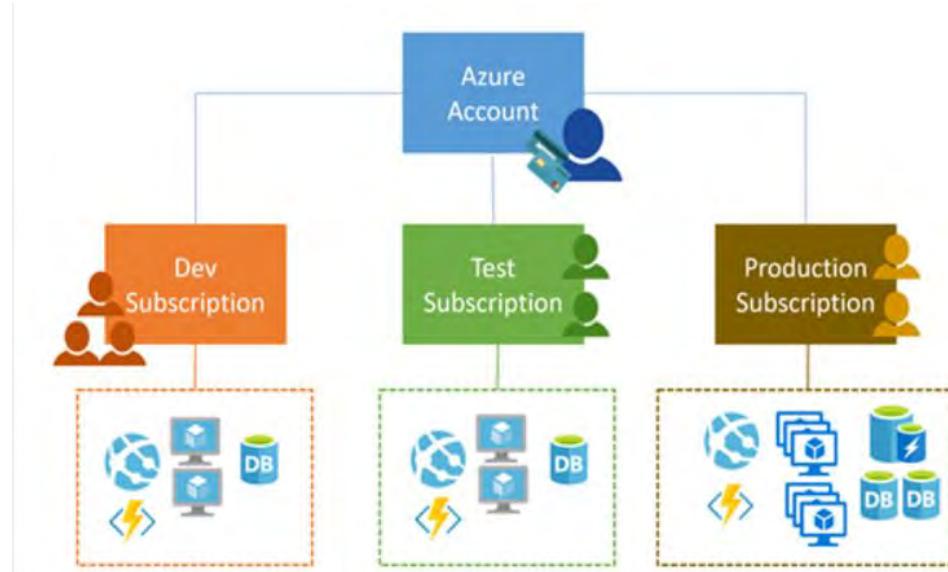
You've reviewed the important considerations about regions and regional pairs. Now think about how you might implement regions in your organization.

- **Consider resource and region deployment.** Plan the regions where you want to deploy your resources. For most Azure services, when you deploy a resource in Azure, you choose the region where you want your resource to be deployed.
- **Consider service support by region.** Research region and service availability. Some services or Azure Virtual Machines features are available only in certain regions, such as **specific Virtual Machines sizes or storage types**.
- **Consider services that don't require regions.** Identify services that don't need region support. Some global Azure services that don't require you to select a region. **These services include Azure Active Directory, Microsoft Azure Traffic Manager, and Azure DNS.**
- **Consider exceptions to region pairing.** Check the Azure website for current region availability and exceptions. If you plan to support the **Brazil South region**, note this region is paired with a region outside its geography. The **Singapore** region also has an exception to standard regional pairing.
- **Consider benefits of data residency.** Take advantage of the benefits of data residency offered by regional pairs. This feature can help you meet requirements for tax and law enforcement jurisdiction purposes.

Subscriptions: Billing unit that aggregate all the costs of the resources that are inside the subscription. Proveen un scope para governanza y seguridad. Podemos tener tantas suscripciones como queramos. Cada suscripcion esta asociada a un solo tenant(Puedes moverlas de tenant), pero un tenant puede tener muchas suscripciones. Hay suscripciones gratis, pay as you go y empresariales

Resource group: is a container that holds related resources for an Azure solution. The resource group can include all the resources for the solution, or only those resources that you want to manage as a group.

Azure AD tenant----Subscription----resource group-----resource



More than one Azure account can be linked to the same subscription

Things to know about obtaining an Azure subscription

Review the following ways to obtain an Azure subscription and consider which options would work for your organization.

Procurement option	Description
	Enterprise agreement Any Enterprise Agreement customer can add Azure to their agreement by making an upfront monetary commitment to Azure. The commitment is consumed throughout the year by using any combination of the wide variety of cloud services Azure offers.
	Microsoft reseller Buy Azure through the Open Licensing program , which provides a simple, flexible way to purchase cloud services from your Microsoft reseller. If you already purchased an Azure in Open license key, activate a new subscription or add more credits now.
	Microsoft partner Find a Microsoft partner who can design and implement your Azure cloud solution. These partners have the business and technology expertise to recommend solutions that meet the unique needs of your business.
	Personal free account Any user can sign up for a free trial account . You can get started using Azure right away, and you won't be charged until you choose to upgrade.

Things to consider when choosing Azure subscriptions

As you think about which types of Azure subscriptions would work for your organization, consider these scenarios:

- Consider trying Azure for free. An Azure free subscription includes a monetary credit to spend on any service for the first 30 days. You get free access to the most popular Azure products for 12 months, and access to more than 25 products that are always free. An Azure free subscription is an excellent way for new users to get started.
 - To set up a free subscription, you need a phone number, a credit card, and a Microsoft account.
 - The credit card information is used for identity verification only. You aren't charged for any services until you upgrade to a paid subscription.
- Consider paying monthly for used services. A Pay-As-You-Go (PAYG) subscription charges you monthly for the services you used in that billing period. This subscription type is appropriate for a wide range of users, from individuals to small businesses, and many large organizations as well.
- Consider using an Azure Enterprise Agreement. An Enterprise Agreement provides flexibility to buy cloud services and software licenses under one agreement. The agreement comes with discounts for new licenses and Software Assurance. This type of subscription targets enterprise-scale organizations.
- Consider supporting Azure for students. An Azure for Students subscription includes a monetary credit that can be used within the first 12 months.
 - Students can select free services without providing a credit card during the sign-up process.
 - You must verify your student status through your organizational email address.

3. Which option preserves data residency, and offers comprehensive compliance and resiliency options?

Azure Active Directory (Azure AD) Account

Regions

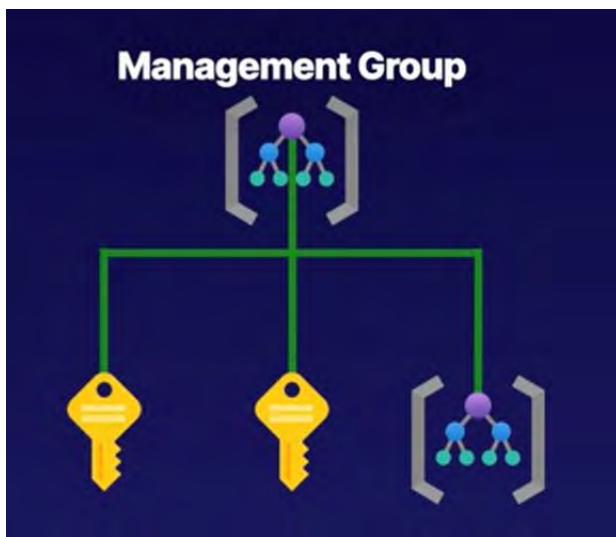
✓ Correct. Regions preserve data residency, and offer comprehensive compliance and resiliency options for customers.

Subscriptions

Management groups

Management groups provide a governance scope above subscriptions.

Nos permiten organizar nuestras suscripciones agrupándolas dentro de estos management groups. El management group que esta mas arriba es el root management group.

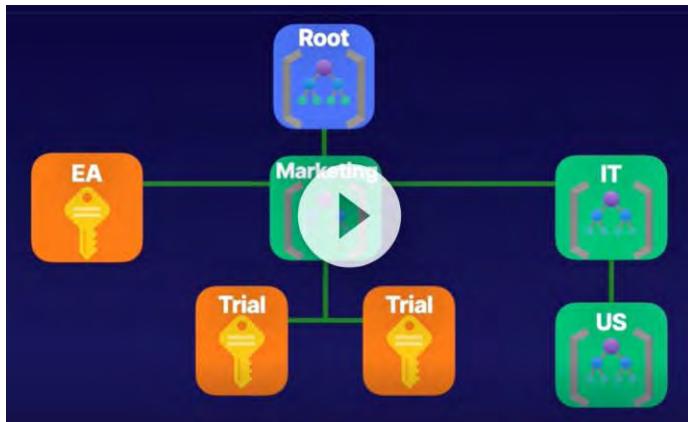


Para poder manejar el root management group se debe tener permisos elevados de user Access administrator (no es dado por default).

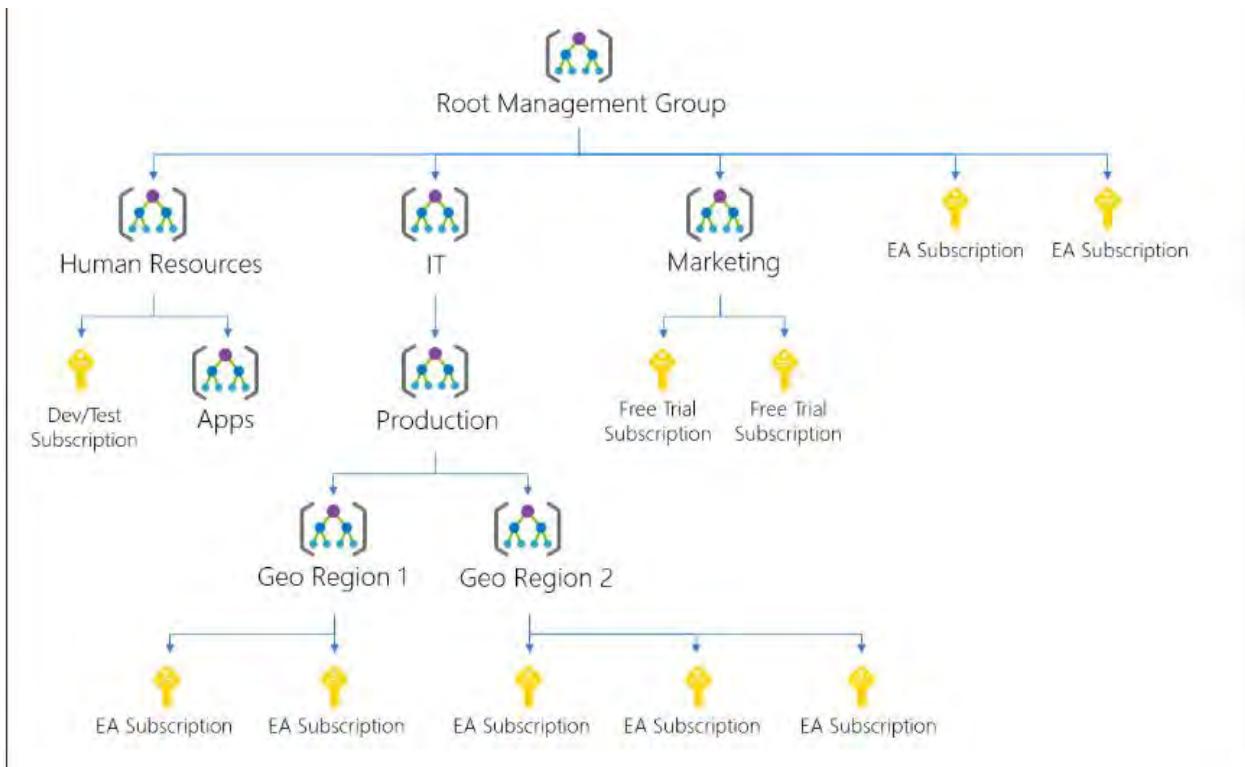
All subscriptions within a management group automatically inherit the conditions applied to that management group.

Azure role-based access control authorization for management group operations isn't enabled by default

Este árbol soporta 6 niveles de jerarquía de management groups y suscripciones.



Puedes aplicar políticas de RBAC por ejemplo en algún management group y esos permisos se darán también a todos sus hijos.



All subscriptions within a management group inherit the conditions applied to the management group.

Azure Policy

Azure Policy helps to enforce organizational standards and to assess compliance at-scale. Through its compliance dashboard, it provides an aggregated view to evaluate the overall state of the environment, with the ability to drill down to the per-resource, per-policy granularity.

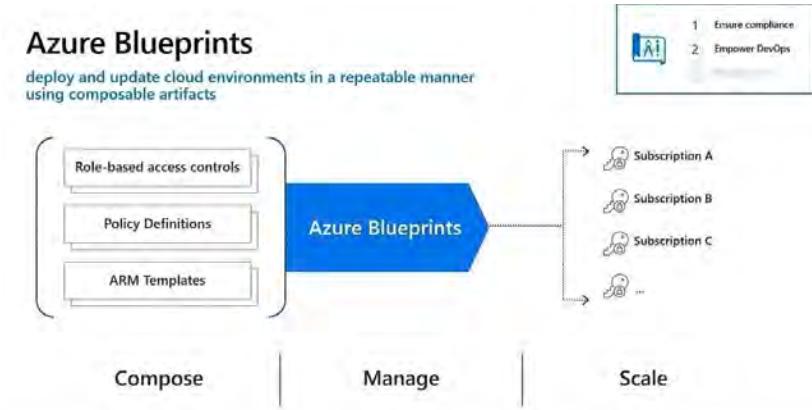
Common use cases for Azure Policy include implementing governance for resource consistency, regulatory compliance, security, cost, and management.

Azure Policy evaluates resources in Azure by comparing the properties of those resources to business rules. These business rules, described in [JSON format](#), are known as [policy definitions](#).

the policy definition or initiative is [assigned](#) to any scope of resources that Azure supports, such as [management groups](#), [subscriptions](#), [resource groups](#), or individual resources.

RBAC focuses on what resources the users can access and the policy is focused on the properties of resources.

Azure blueprints es como arm templates pero en grande ya que te permite migrar todo un ambiente de azure en blueprints.



Blueprint definition

A blueprint is composed of *artifacts*. Azure Blueprints currently supports the following resources as artifacts:

Resource	Hierarchy options	Description
Resource Groups	Subscription	Create a new resource group for use by other artifacts within the blueprint. These placeholder resource groups enable you to organize resources exactly the way you want them structured and provides a scope limiter for included policy and role assignment artifacts and ARM templates.
ARM template	Subscription, Resource Group	Templates, including nested and linked templates, are used to compose complex environments. Example environments: a SharePoint farm, Azure Automation State Configuration, or a Log Analytics workspace.
Policy Assignment	Subscription, Resource Group	Allows assignment of a policy or initiative to the subscription the blueprint is assigned to. The policy or initiative must be within the scope of the blueprint definition location. If the policy or initiative has parameters, these parameters are assigned at creation of the blueprint or during blueprint assignment.
Role Assignment	Subscription, Resource Group	Add an existing user or group to a built-in role to make sure the right people always have the right access to your resources. Role assignments can be defined for the entire subscription or nested to a specific resource group included in the blueprint.

Azure policy tiene:

- policy definition: que define la evaluation criteria for compliance y define las acciones a tomar así sea auditar o denegar
- Policy Assignment: el scope al que asignaremos nuestra política(management group, suscripción, resource group, resource)
- Initiative definition: collection of policies que quieren lograr un objetivo singular

Ejemplo:



Ejemplo de un policy:

This screenshot shows the 'Allowed locations' policy definition in the Azure portal. The top navigation bar includes 'Home', 'Policy', and 'cloud_user_p_aa7fa7ee...'. The main area shows the JSON code for the policy definition, which restricts allowed locations to specific regions. A large play button icon is overlaid on the code area.

```
1  {
2    "properties": {
3      "displayName": "Allowed locations",
4      "policyType": "Builtin",
5      "mode": "Indexed",
6      "description": "This policy enables you to restrict the locations your organization can specify when deploying resources. Use to enforce your geo-compliance requirements or to prevent deployment to specific regions.", // This line is partially obscured by a play button
7      "metadata": {
8        "version": "1.0.0",
9        "category": "General"
10      },
11      "parameters": {
12        "listOfAllowedLocations": {
13          "type": "Array",
14          "metadata": {
15            "description": "The list of locations that can be specified when deploying resources.",
16            "strongType": "location",
17            "displayName": "Allowed locations"
18          }
19        }
20      }
21    }
22  }
```

This slide summary highlights the key features of Azure Policy. It includes icons for 'Policy Definition' (yellow document) and 'Policy Assignment' (blue document). A callout bubble on the right lists four main benefits:

- Create, Manage, and Assign policies
- Enforce compliance on resources
- Audit compliance
- Deny creation of resources outside of compliance

Things to know about Azure Policy

The main advantages of Azure Policy are in the areas of enforcement and compliance, scaling, and remediation. Azure Policy is also important for teams that run an environment that requires different forms of governance.

Advantage	Description
Enforce rules and compliance	Enable built-in policies, or build custom policies for all resource types. Support real-time policy evaluation and enforcement, and periodic or on-demand compliance evaluation.
Apply policies at scale	Apply policies to a management group with control across your entire organization. Apply multiple policies and aggregate policy states with policy initiative. Define an exclusion scope.
Perform remediation	Conduct real-time remediation, and remediation on your existing resources.
Exercise governance	Implement governance tasks for your environment: <ul style="list-style-type: none">- Support multiple engineering teams (deploying to and operating in the environment)- Manage multiple subscriptions- Standardize and enforce how cloud resources are configured- Manage regulatory compliance, cost control, security, and design consistency

Things to consider when using Azure Policy

Review the following scenarios for using Azure Policy. Consider how you can implement the service in your organization.

- Consider **deployable resources**. Specify the resource types that your organization can deploy by using Azure Policy. You can specify the set of virtual machine SKUs that your organization can deploy.
- Consider **location restrictions**. Restrict the locations your users can specify when deploying resources. You can choose the geographic locations or regions that are available to your organization.
- Consider **rules enforcement**. Enforce compliance rules and configuration options to help manage your resources and user options. You can enforce a required tag on resources and define the allowed values.
- Consider **inventory audits**. Use Azure Policy with Azure Backup service on your VMs and run inventory audits.

There are four basic steps to create and work with policy definitions in Azure Policy.

Step 1: Create policy definitions

A policy definition expresses a condition to evaluate and the actions to perform when the condition is met. You can create your own policy definitions, or choose from built-in definitions in Azure Policy. You can create a policy definition to prevent VMs in your organization from being deployed, if they're exposed to a public IP address.

Step 2: Create an initiative definition

An initiative definition is a set of policy definitions that help you track your resource compliance state to meet a larger goal. You can create your own initiative definitions, or use built-in definitions in Azure Policy. You can use an initiative definition to ensure resources are compliant with security regulations.

Step 3: Scope the initiative definition

Azure Policy lets you control how your initiative definitions are applied to resources in your organization. You can limit the scope of an initiative definition to specific management groups, subscriptions, or resource groups.

Step 4: Determine compliance

After you assign an initiative definition, you can evaluate the state of compliance for all your resources. Individual resources, resource groups, and subscriptions within a scope can be exempted from having the policy rules affect it. Exclusions are handled individually for each assignment.

Tagging resources

Tags sirven para etiquetar recursos por ejemplo Name:value, dept:marketing, Env:Prod, el nombre puede tener hasta 512 caracteres y el valor 256. Storage accounts can only have a name with 128 characters.

Si tageas una suscripción o un resource group, los recursos que estén dentro de ella no heredaran esta etiqueta

Un recurso o resource group puede tener hasta 50 tags

Ejemplos de querys en powershell usando etiquetas:

```
PS /home/cloud> az resource list --tag project=az104 --query [].name -o tsv
tagged-vm
tagged-vmVMNic
tagged-vmNSG
tagged-vmPublicIP
PS /home/cloud> az resource list --tag project=az104 --query [].id -o tsv
/subscriptions/0f39574d-d756-48cf-b622-0e27a6943bd2/resourceGroups/1-57d65813-playground-sandbox/providers/Microsoft.Compute/vm
hines/tagged-vm
/subscriptions/0f39574d-d756-48cf-b622-0e27a6943bd2/resourceGroups/1-57d65813-playground-sandbox/providers/Microsoft.Network/ne
rfaces/tagged-vmVMNic
/subscriptions/0f39574d-d756-48cf-b622-0e27a6943bd2/resourceGroups/1-57d65813-playground-sandbox/providers/Microsoft.Network/ne
urityGroups/tagged-vmNSG
/subscriptions/0f39574d-d756-48cf-b622-0e27a6943bd2/resourceGroups/1-57d65813-playground-sandbox/providers/Microsoft.Network/p
addresses/tagged-vmPublicIP
PS /home/cloud>
```



Manage resources via tags. For example, shutting down all VMs with a specific tag.



Tags are not inherited from the higher scope like a resource group. Each resource must be tagged.

Locking and moving resources

Locks: allow you to override permissions to resources, can lock subscriptions, resource groups or resources.

Lock restrictions apply to all users and roles.

Lock Types:

Lock Types



- ReadOnly allows authorized users to read a resource, but they cannot delete or update the resource
- CanNotDelete allows authorized users to read and modify a resource, but they cannot delete the resource
- Locks are inherited from the parent scope

Can move resources between suscripcions and resources groups

Home > CreateVm-canonical.0001-com-ubuntu-server-local-2-2021062134613 > lockdemo-vm

lockdemo-vm | Locks

Virtual machine

Search (Cmd+)

+ Add Resource group Subscription Refresh

Connect

Disks

Size

Security

Adviser recommendations

Extensions

Continuous delivery

Availability + scaling

Configuration

Identity

Properties

Locks

This resource has no locks.

Play button

Add Resource group Subscription Refresh

Add lock

Lock name:

Lock type:

Notes:

Delete

Play button

Can't delete a storage account if a resource has a lock

To move resources you have to go to the resource group:

Add Edit columns Delete resource group Refresh Export to CSV Open query Feedback Open in mobile ...

^ Essentials

Subscription (change) P2-Real Hands-On Labs

Subscription ID 964df7ca-3ba4-48b6-a695-1ed9db5723f8

Tags (change) Click here to add tags

Filter for any field... Type == all Add filter

Deployment 3 Succeeded

Location West US

Move to another resource group

Move to another subscription

Move to another region

Assign tags View

Move

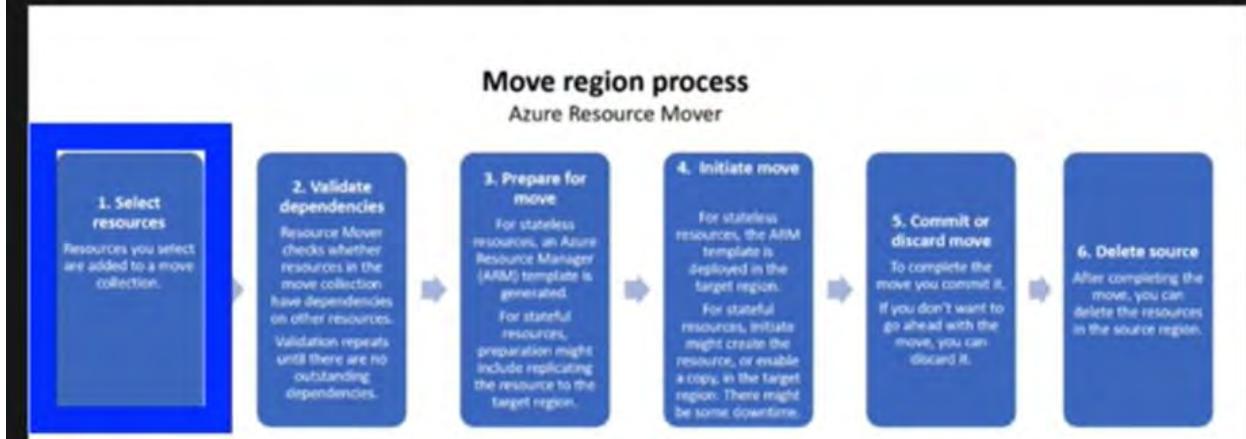
Delete

Export template

Play button

Move region process:

Move region process



LOCKING AND MOVING RESOURCES

Moving Resources



Considerations

Supported Resources



Virtual Machines



Storage Accounts



Virtual Networks

Unsupported Resources



Azure Active Directory Domain Services



Azure Backup Vaults



Azure App Service Gateways

Managing Azure Costs

MANAGING AZURE COSTS

What Affects Cost?

Subscription Type

Free, pay-as-you-go, Enterprise Agreement, and Cloud Solution Provider (CSP)

Resource Type

For example, storage account Blob storage vs. table storage

Usage Meters

Utilities like overall CPU time, ingress/egress network traffic, and disk size

Resource Usage

The costs of actually using a resource

Location

The costs for various services vary across geographical regions

Cost Best Practices and Tools

Best Practices

-  Select appropriate resource for use case
-  Understand resource needs (sizing)
-  Deallocate resources when not needed
-  Use cloud capabilities where possible (Scalability, Elasticity)
-  Plan costs prior to purchase

Cost Tools



Pricing Calculator



Total Cost of Ownership (TCO) Calculator



Cost Management

Pricing calculator puedes ver el costo de los recursos de azure para estimarlos, TCO es para comparar costos on-prem y en la nube y en cost management puedes ver los gastos en la nube así como crear alertas.

Para crear la alerta primero debes crear un Budget donde pondrás lo que tienes para gastar



Pricing Calculator
Estimate workload costs for prospective workloads



TCO Calculator
Compare costs to determine cost savings between on-premises and cloud solutions



Cost Management
Analyze costs, apply filtering, and create budgets

Apply cost savings

✓ 100 XP

2 minutes

Azure has several options that can help you gain significant cost savings for your organization. As you prepare your implementation plan for Azure subscriptions, services, and resources, consider the following cost saving advantages.

Cost saving	Description
Reservations	Save money by paying ahead. You can pay for one year or three years of virtual machine, SQL Database compute capacity, Azure Cosmos DB throughput, or other Azure resources. Pre-paying allows you to get a discount on the resources you use. Reservations can significantly reduce your virtual machine, SQL database compute, Azure Cosmos DB, or other resource costs up to 72% on pay-as-you-go prices. Reservations provide a billing discount and don't affect the runtime state of your resources.
Azure Hybrid Benefits	Access pricing benefits if you have a license that includes <i>Software Assurance</i> . Azure Hybrid Benefits helps maximize the value of existing on-premises Windows Server or SQL Server license investments when migrating to Azure. There's an Azure Hybrid Benefit Savings Calculator to help you determine your savings.
Azure Credits	Use the monthly credit benefit to develop, test, and experiment with new solutions on Azure. As a Visual Studio subscriber, you could use Microsoft Azure at no extra charge. With your monthly Azure credit, Azure is your personal sandbox for development and testing.
Azure regions	Compare pricing across regions. Pricing can vary from one region to another, even in the US. Double check the pricing in various regions to see if you can save by selecting a different region for your subscription.
Budgets	Apply the budgeting features in Microsoft Cost Management to help plan and drive organizational accountability. With budgets, you can account for the Azure services you consume or subscribe to during a specific period. Monitor spending over time and inform others about their spending to proactively manage costs. Use budgets to compare and track spending as you analyze costs.
Pricing Calculator	The Pricing Calculator provides estimates in all areas of Azure, including compute, networking, storage, web, and databases.

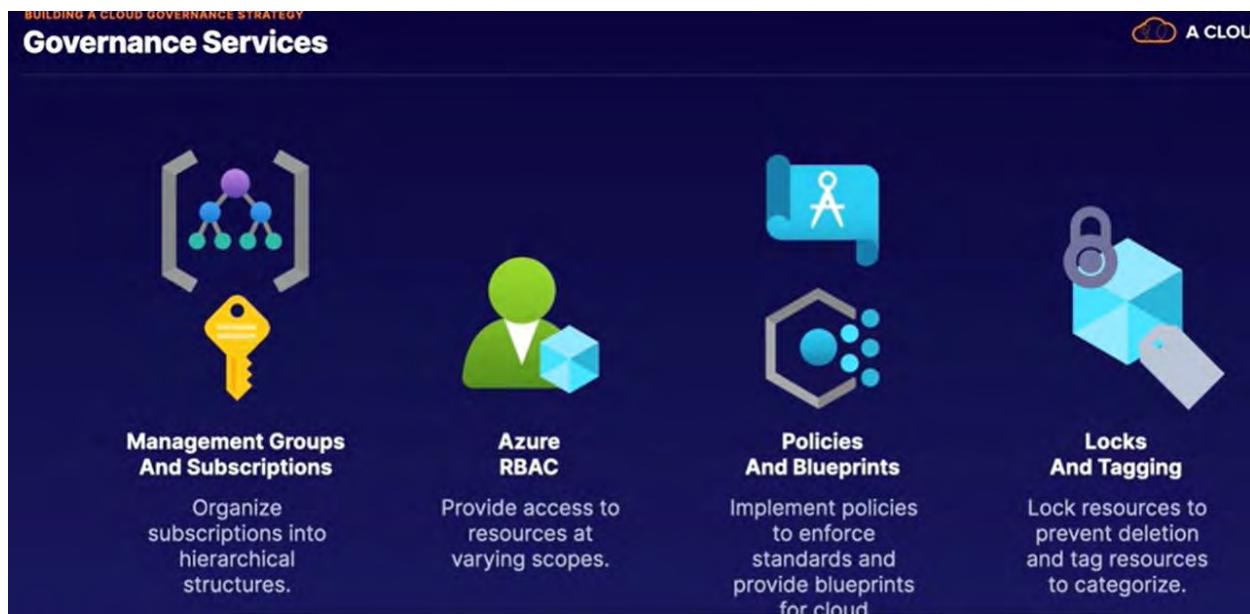
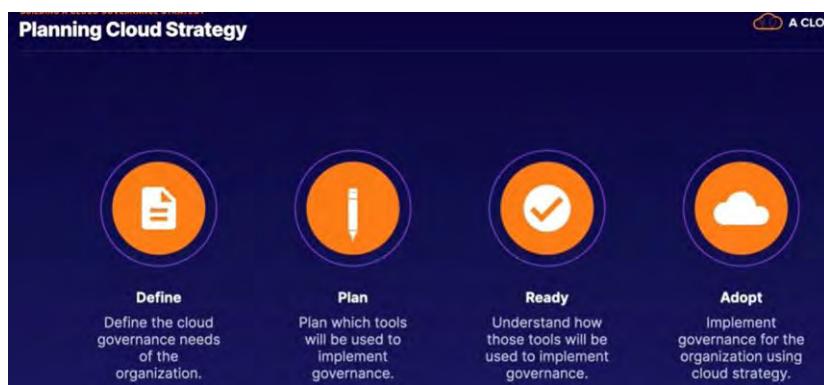
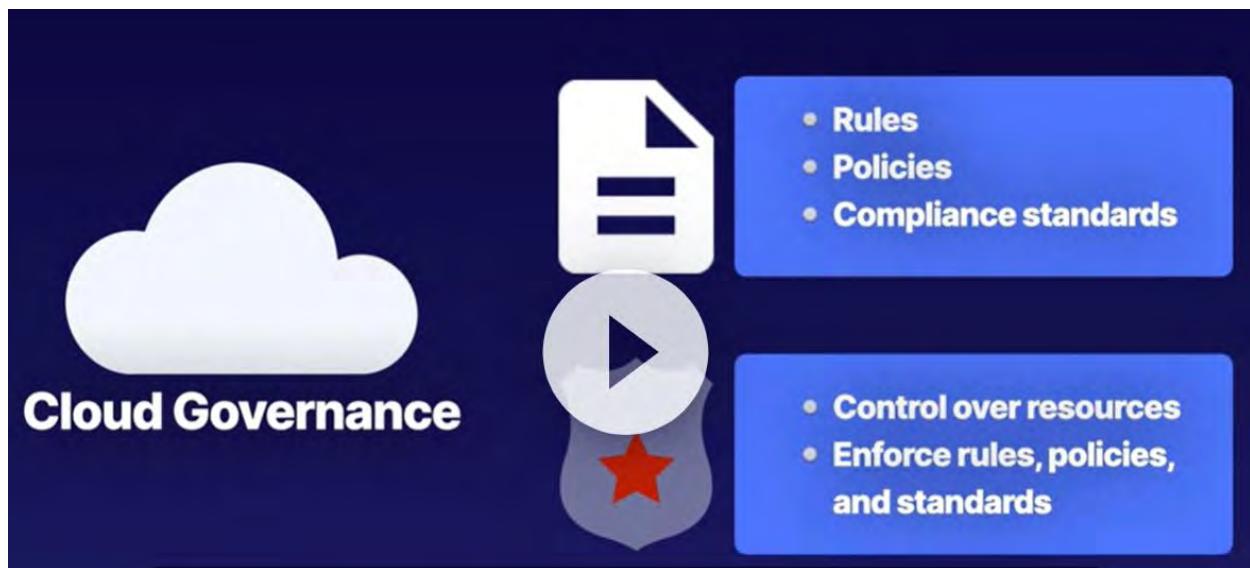
Things to consider when using Microsoft Cost Management

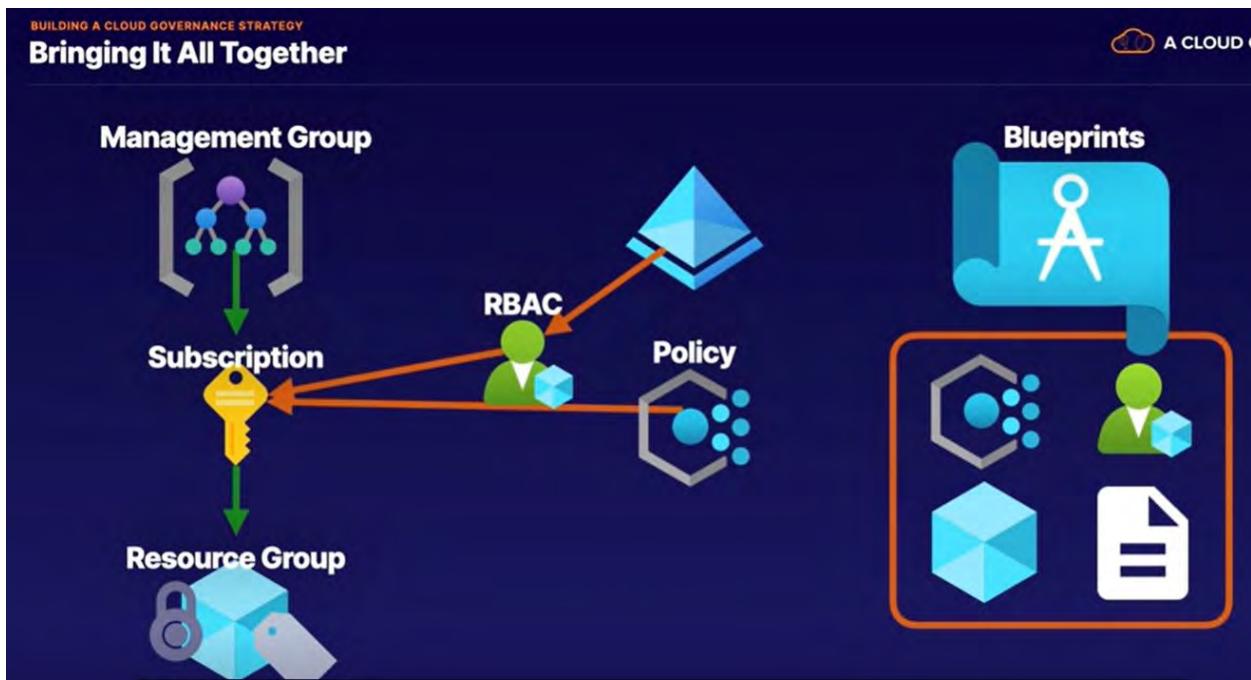
Microsoft Cost Management can help you plan for and control your organization costs. Consider how the product features can be implemented to support your business scenarios:

- Consider cost analysis. Take advantage of Microsoft Cost Management cost analysis features to explore and analyze your organizational costs. You can view aggregated costs by organization to understand where costs are accrued, and to identify spending trends. Monitor accumulated costs over time to estimate monthly, quarterly, or even yearly cost trends against a budget.
- Consider budget options. Use Microsoft Cost Management features to establish and maintain budgets. The product helps you plan for and meet financial accountability in your organization. Budgets help prevent cost thresholds or limits from being surpassed. You can utilize analysis data to inform others about their spending to proactively manage costs. The budget features help you see how company spending progresses over time.
- Consider recommendations. Review the Microsoft Cost Management recommendations to learn how you can optimize and improve efficiency by identifying idle and underutilized resources. Recommendations can reveal less expensive resource options. When you act on the recommendations, you change the way you use your resources to save money. Using recommendations is an easy process:
 1. View cost optimization recommendations to see potential usage inefficiencies.
 2. Act on a recommendation to modify your Azure resource use and implement a more cost-effective option.
 3. Verify the new action to make sure the change has the desired effect.
- Consider exporting cost management data. Microsoft Cost Management helps you work with your billing information. If you use external systems to access or review cost management data, you can easily export the data from Azure.
 - Set a daily scheduled export in comma-separated-value (CSV) format and store the data files in Azure storage.
 - Access your exported data from your external system.

Building a cloud governance strategy

Governance: manner of controlling and the means and methods by which we control something

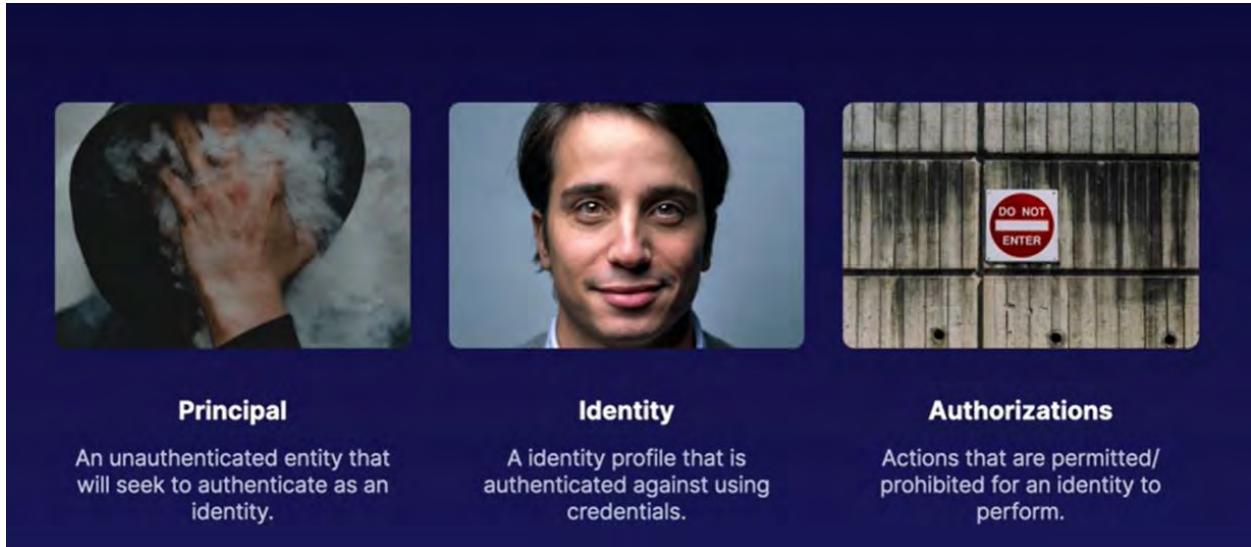




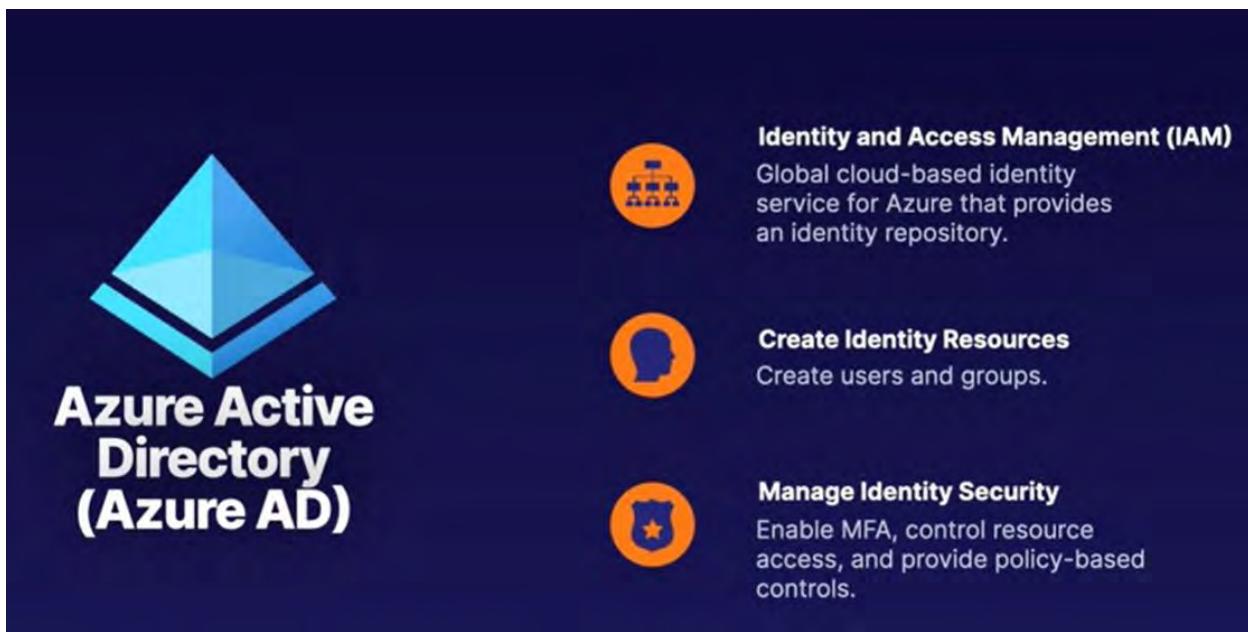
Blueprints es como un ARM template para empacar en un solo archivo todas estas cosas de gobernanza

Conceptualizing Azure Active Directory

IAM (Identity and Access management) basics:



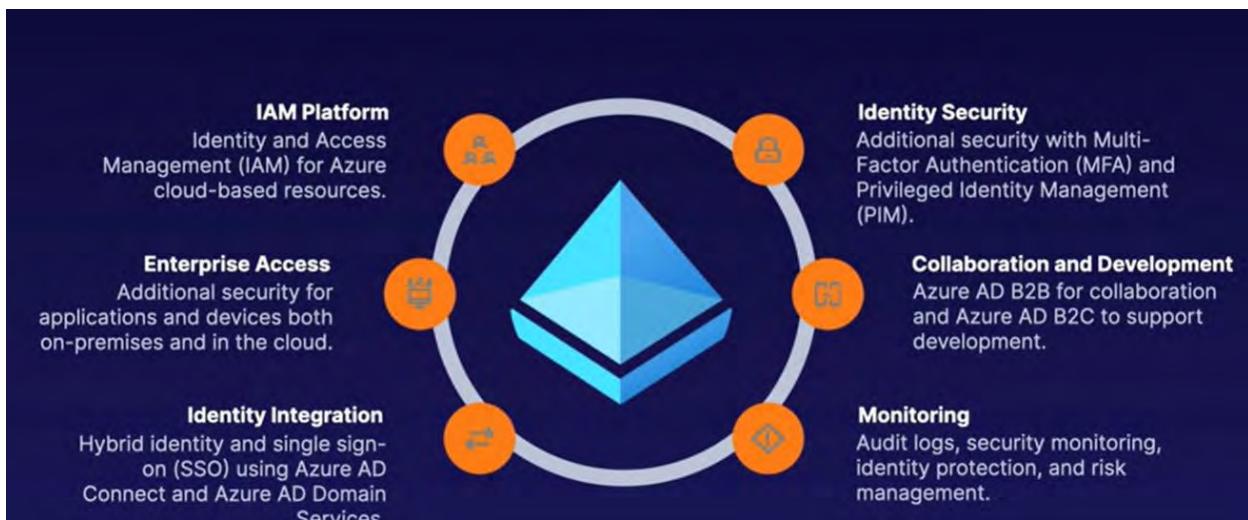
Azure Active Directory is the IAM service in Azure



Organization=AD Tenant=Azure AD

Podemos recibir dominios genericos de azure o también personalizados

Azure AD características:

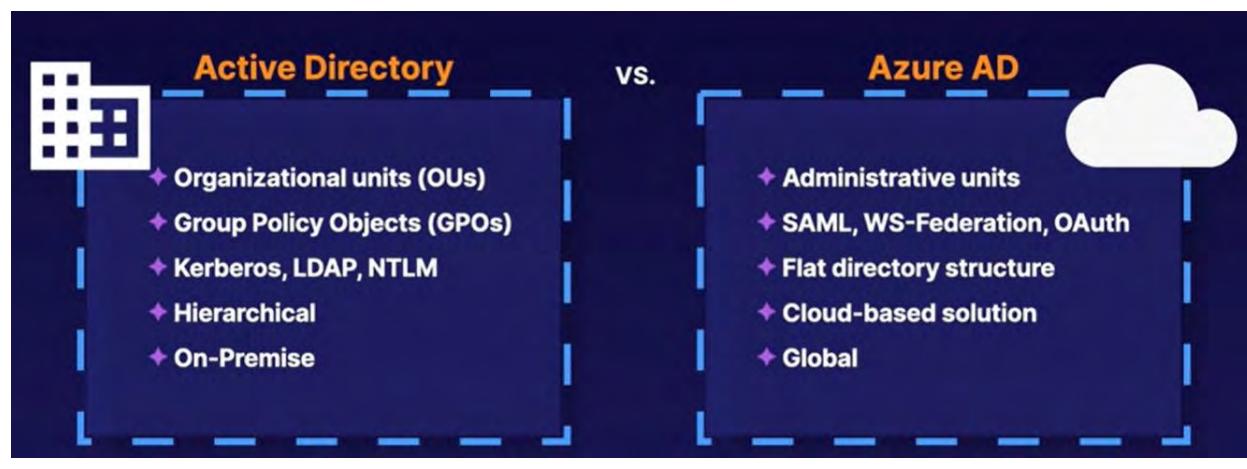


Licencias de Azure:

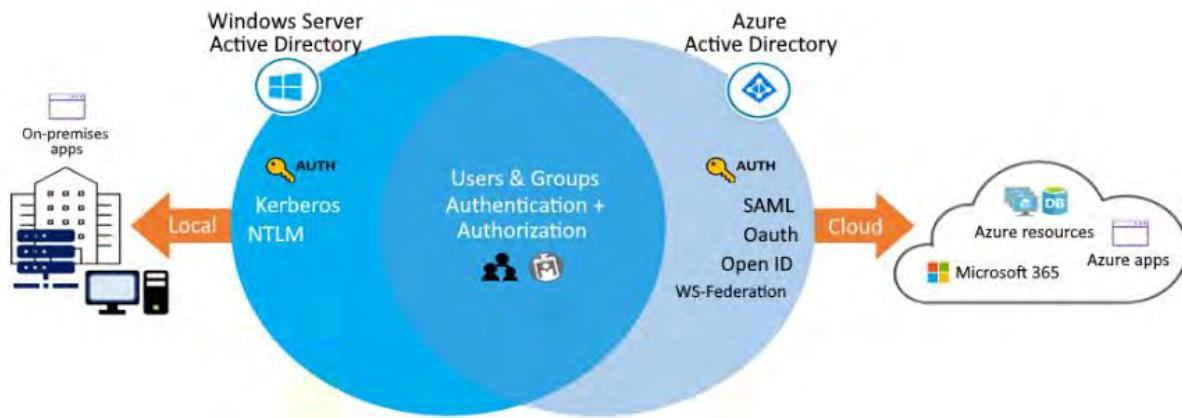
Azure Licensing Features

Feature	Free	Office 365	Premium P1	Premium P2
Directory Objects	500,000	Unlimited	Unlimited	Unlimited
SSO (Single Sign-On)	Unlimited	Unlimited	Unlimited	Unlimited
Core IAM	✓	✓	✓	✓
B2B Collaboration	✓	✓	✓	✓
IAM for O365		✓	✓	✓
Premium Features			✓	✓
Hybrid Identities			✓	✓
Dynamic Groups			✓	✓
Conditional Access			✓	✓
Identity Protection				✓
Identity Governance				✓

Diferencias entre Active directory y Azure AD:



Note: Microsoft cloud-based offerings that use Azure AD for IAM include Azure, Microsoft 365, Microsoft Intune, and Microsoft Dynamics 365



Things to know about Azure AD features

Let's examine some of the prominent features of Azure AD.

Azure AD feature	Description
Single sign-on (SSO) access	Azure AD provides secure single sign-on (SSO) to web apps on the cloud and to on-premises apps. Users can sign in with the same set of credentials to access all their apps.
Ubiquitous device support	Azure AD works with iOS, macOS, Android, and Windows devices, and offers a common experience across the devices. Users can launch apps from a personalized web-based access panel, mobile app, Microsoft 365, or custom company portals by using their existing work credentials.
Secure remote access	Azure AD enables secure remote access for on-premises web apps. Secure access can include multifactor authentication (MFA), conditional access policies, and group-based access management. Users can access on-premises web apps from everywhere, including from the same portal.
Cloud extensibility	Azure AD can extend to the cloud to help you manage a consistent set of users, groups, passwords, and devices across environments.
Sensitive data protection	Azure AD offers unique identity protection capabilities to secure your sensitive data and apps. Admins can monitor for suspicious sign-in activity and potential vulnerabilities in a consolidated view of users and resources in the directory.
Self-service support	Azure AD lets you delegate tasks to company employees that might otherwise be completed by admins with higher access privileges. Providing self-service app access and password management through verification steps can reduce helpdesk calls and enhance security.

Describe Azure Active Directory concepts

100 XP

2 minutes

To implement Azure Active Directory in your corporate configuration, you need to understand the key components of the service. The following table describes the main components and concepts of Azure AD and explains how they work together to support service features.

Azure AD concept	Description
Identity	An <i>identity</i> is an object that can be authenticated. The identity can be a user with a username and password. Identities can also be applications or other servers that require authentication by using secret keys or certificates. Azure AD is the underlying product that provides the identity service.
Account	An <i>account</i> is an identity that has data associated with it. To have an account, you must first have a valid identity. You can't have an account without an identity.
Azure AD account	An <i>Azure AD account</i> is an identity that's created through Azure AD or another Microsoft cloud service, such as Microsoft 365. Identities are stored in Azure AD and are accessible to your organization's cloud service subscriptions. The Azure AD account is also called a <i>work or school account</i> .
Azure tenant (directory)	An Azure <i>tenant</i> is a single dedicated and trusted instance of Azure AD. Each tenant (also called a <i>directory</i>) represents a single organization. When your organization signs up for a Microsoft cloud service subscription, a new tenant is automatically created. Because each tenant is a dedicated and trusted instance of Azure AD, you can create multiple tenants or instances.
Azure subscription	An Azure subscription is used to pay for Azure cloud services. Each subscription is joined to a single tenant. You can have multiple subscriptions.

Things to consider when using Azure AD rather than AD DS

Azure AD is similar to AD DS, but there are significant differences. It's important to understand that using Azure AD for your configuration is different from deploying an Active Directory domain controller on an Azure virtual machine and then adding it to your on-premises domain.

As you plan your identity strategy, consider the following characteristics that distinguish Azure AD from AD DS.

- **Identity solution:** AD DS is primarily a directory service, while Azure AD is a full identity solution. Azure AD is designed for internet-based applications that use HTTP and HTTPS communications. The features and capabilities of Azure AD support target strong identity management.
- **Communication protocols:** Because Azure AD is based on HTTP and HTTPS, it doesn't use Kerberos authentication. Azure AD implements HTTP and HTTPS protocols, such as SAML, WS-Federation, and OpenID Connect for authentication (and OAuth for authorization).
- **Federation services:** Azure AD includes federation services, and many third-party services like Facebook.
- **Flat structure:** Azure AD users and groups are created in a flat structure. There are no organizational units (OUs) or group policy objects (GPOs).
- **Managed service:** Azure AD is a managed service. You manage only users, groups, and policies. If you deploy AD DS with virtual machines by using Azure, you manage many other tasks, including deployment, configuration, virtual machines, patching, and other backend processes.

Consider the following features that distinguish the different editions of Azure AD. After you review the features and descriptions, think about which edition works best for your organization. An X indicates the feature is supported.

Feature	Free	Microsoft 365 Apps	Premium P1	Premium P2
Directory Objects	500,000	Unlimited	Unlimited	Unlimited
Single Sign-on	Unlimited	Unlimited	Unlimited	Unlimited
Core Identity and Access Management	X	X	X	X
Business-to-business Collaboration	X	X	X	X
Identity and Access Management for Microsoft 365 apps		X	X	X
Premium Features			X	X
Hybrid Identities			X	X
Advanced Group Access Management			X	X
Conditional Access			X	X
Identity Protection				X
Identity Governance				X

Things to know about the Azure AD join feature

Let's look at some of the benefits of using joined devices:

Benefit	Description
Single-Sign-On (SSO)	Joined devices offer SSO access to your Azure-managed SaaS apps and services. Your users won't have extra authentication prompts when they access work resources. The SSO functionality is available even when users aren't connected to the domain network.
Enterprise state roaming	Starting in Windows 10, your users can securely synchronize their user settings and app settings data to joined devices. Enterprise state roaming reduces the time to configure a new device.
Access to Microsoft Store for Business	When your users access Microsoft Store for Business by using an Azure AD account, they can choose from an inventory of applications pre-selected by your organization.
Windows Hello	Provide your users with secure and convenient access to work resources from joined devices.
Restriction of access	Restrict user access to apps from only joined devices that meet your compliance policies.
Seamless access to on-premises resources	Joined devices have seamless access to on-premises resources, when the device has line of sight to the on-premises domain controller.

Things to know about the Azure AD SSPR feature

Examine the following characteristics and requirements of the SSPR feature:

- SSPR requires an Azure AD account with Global Administrator privileges to manage SSPR options. This account can always reset their own passwords, no matter what options are configured.
- SSPR uses a security group to limit the users who have SSPR privileges.
- All user accounts in your organization must have a valid license to use SSPR.
- Consider who can reset their passwords. Decide which users in your organization should be enabled to use the feature. In the Azure portal, there are three options for the SSPR feature: None, Selected, and All.

The screenshot shows the 'Password reset - Properties' page in the Azure Active Directory portal. The left sidebar has 'Manage' and 'Properties' tabs, with 'Properties' selected. The main area shows 'Self service password reset enabled' with three options: 'None', 'Selected', and 'All'. The 'All' option is highlighted with a purple background. A note below says: 'These settings only apply to end users in your organization. Admins are always enabled and are required to use two authentication methods for self-service password reset to reset their password. Click here to learn more about administrator password policies.'

The Selected option is useful for creating specific groups who have SSPR enabled. You can create groups for testing or proof of concept before applying the feature to a larger group. When you're ready to deploy SSPR to all user accounts in your Azure AD tenant, you can change the setting.

- Consider your authentication methods. Determine how many authentication methods are required to reset a password, and select the authentication options for users.
 - Your system must require at least one authentication method to reset a password.
 - A strong SSPR plan offers multiple authentication methods for the user. Options include email notification, text message, or a security code sent to the user's mobile or office phone. You can also offer the user a set of security questions.
 - You can require security questions to be registered for the users in your Azure AD tenant.
 - You can configure how many correctly answered security questions are required for a successful password reset.
- Consider combining methods for stronger security. Security questions can be less secure than other authentication methods. Some users might know the answers for a particular user's questions, or the questions might be easy to solve. If you support security questions, combine this option with other authentication methods.

1. Which choice correctly describes Azure Active Directory?

- Azure AD can be queried through LDAP.
 - Azure AD is primarily an identity solution.
- ✓ Correct. Azure AD is primarily an identity solution. It's designed for internet-based applications by using HTTP and HTTPS communications.
- Azure AD uses organizational units (OUs) and group policy objects (GPOs).

2. What term defines a dedicated and trusted instance of Azure Active Directory?

- Azure tenant
- ✓ Correct. A tenant is a dedicated and trusted instance of Azure AD. A tenant is automatically created when an organization signs up for a Microsoft cloud service subscription.
- Identity
 - Azure AD account

3. Your users want to sign-in to devices, apps, and services from anywhere. Users want to sign-in by using an organizational work or school account instead of a personal account. What should you do first?

- Enable the device in Azure AD.
 - Join the device to Azure AD.
- ✓ Correct. Joining the device provides the features you need.
- Register the device with Azure AD.

Managing tenants



Azure Active Directory (B2C)

Azure Active Directory (B2C)

Choose Azure Active Directory (B2C) if you need to:

Provide highly customizable sign-in and other identity management experiences for your external facing applications. [Learn more](#)

Scale up to hundreds of millions of users. [Learn more](#)

Creating and managing users

Types of users:

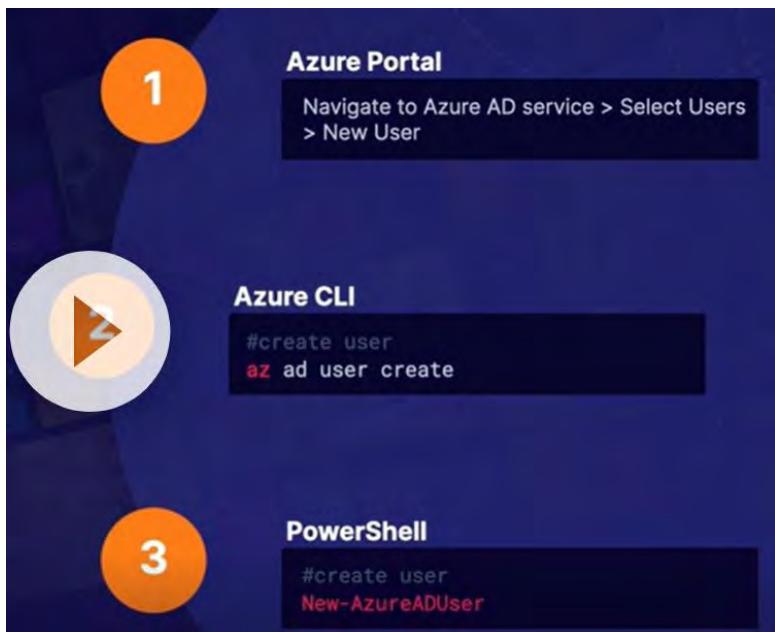
		
Administrators	Members	Guests
Users with an administrator role assigned.	Regular users that are native to Azure AD.	External users that are invited to the Azure AD Tenant.



- Members have default permissions
- These identities are JSON objects
- Each user can have role assignments
- Each user can have object ownership

```
{
  "accountEnabled": true,
  "department": "Student",
  "displayName": "Eruza Duolc",
  "studentId": "0123456",
  "givenName": "Eruza",
  "jobTitle": "Student",
  "objectType": "User",
  "surname": "Duolc",
  "usageLocation": "US",
  "userPrincipalName": "eruzaduolc@contoso.com",
  "userType": "Member"
}
```

Para crearlos podemos usar el azure portal, azure cli y powershell



Things to know about user accounts

The following table describes the user accounts supported in Azure AD. As you review these options, consider what types of user accounts suit your organization.

User account	Description
Cloud identity	A user account with a <i>cloud identity</i> is defined only in Azure AD. This type of user account includes administrator accounts and users who are managed as part of your organization. A cloud identity can be for user accounts defined in your Azure AD organization, and also for user accounts defined in an external Azure AD instance. When a cloud identity is removed from the primary directory, the user account is deleted.
Directory-synchronized identity	User accounts that have a <i>directory-synchronized identity</i> are defined in an on-premises Active Directory. A synchronization activity occurs via Azure AD Connect to bring these user accounts in to Azure. The source for these accounts is Windows Server Active Directory.
Guest user	<i>Guest user accounts</i> are defined outside Azure. Examples include user accounts from other cloud providers, and Microsoft accounts like an Xbox LIVE account. The source for guest user accounts is Invited user. Guest user accounts are useful when external vendors or contractors need access to your Azure resources.

Information and settings that describe a user are stored in the user account profile.

- The profile can have other settings like a user's job title, and their contact email address.
- A user with Global administrator or User administrator privileges can preset profile data in user accounts, such as the main phone number for the company.
- Non-admin users can set some of their own profile data, but they can't change their display name or account name.

Things to consider when managing cloud identity accounts

There are several points to consider about managing user accounts. As you review this list, consider how you can add cloud identity user accounts for your organization.

- Consider user profile data. Allow users to set their profile information for their accounts, as needed. User profile data, including the user's picture, job, and contact information is optional. You can also supply certain profile settings for each user based on your organization's requirements.
- Consider restore options for deleted accounts. Include restore scenarios in your account management plan. Restore operations for a deleted account are available up to 30 days after an account is removed. After 30 days, a deleted user account can't be restored.
- Consider gathered account data. Collect sign-in and audit log information for user accounts. Azure AD lets you gather this data to help you analyze and improve your infrastructure.

Creating and managing groups

CREATING AND MANAGING GROUPS

Describing Groups

Owner and Members
An owner of the group or a member of the group

Type of Group
A security group or a Microsoft 365 group

Membership Type
Assigned, dynamic user, or dynamic device

Key Takeaways

Group Types



Security

Security groups are used to manage access to shared resources for a group of users.



Microsoft 365

Microsoft 365 groups are used to give members access to a shared mailbox, calendar, files, etc.

Membership Types



Assigned

Users are specifically selected to be members of a group.



Dynamic User

Membership rules are created that automate group membership via user attributes.



Dynamic Device

Membership rules are created that automate group membership via device attributes.

- Use security groups to set permissions for all group members at the same time, rather than adding permissions to each member individually.
- Add Microsoft 365 groups to enable group access for guest users outside your Azure AD organization.
- Security groups can be implemented only by an Azure AD administrator.
- Normal users and Azure AD admins can both use Microsoft 365 groups.

Things to consider when adding group members

When you add members to a group, there are different ways you can assign member access rights. As you read through these options, consider which groups are needed to support your organization, and what access rights should be applied to group members.

Access rights	Description
Assigned	Add specific users as members of a group, where each user can have unique permissions.
Dynamic user	Use dynamic membership rules to automatically add and remove group members. When member attributes change, Azure reviews the dynamic group rules for the directory. If the member attributes meet the rule requirements, the member is added to the group. If the member attributes no longer meet the rule requirements, the member is removed.
Dynamic device	(Security groups only) Apply dynamic group rules to automatically add and remove devices in security groups. When device attributes change, Azure reviews the dynamic group rules for the directory. If the device attributes meet the rule requirements, the device is added to the security group. If the device attributes no longer meet the rule requirements, the device is removed.

Creating Administrative Units

Sirven para que el scope de un admin no sea en toda la organización, si no solo en el scope que se defina para una administrative unit.

Administrative units restrict permissions in a role to any portion of your organization that you define. You could, for example, use administrative units to delegate the [Helpdesk Administrator](#) role to regional support specialists, so they can manage users only in the region that they support.

Puedes tener administrative units por región, por unidad de negocio

Al añadir una administrative unit tienes estas opciones de roles:

The screenshot shows the 'Add administrative unit' page with the 'Assign roles' tab selected. The 'Properties' tab is also visible. The 'Administrative roles' section contains the following table:

Role	Description	Type
Authentication administrator	Has access to view, set, and reset authentication methods for users and groups.	Built-in
Groups administrator	Can manage all aspects of groups and group settings.	Built-in
Helpdesk administrator	Can reset passwords for non-administrators and Helpdesk users.	Built-in
License administrator	Ability to assign, remove and update license assignments.	Built-in
Password administrator	Can reset passwords for non-administrators and Password administrators.	Built-in
User administrator	Can manage all aspects of users and groups, including user creation and deletion.	Built-in

Si asignas un grupo a una administrative unit los miembros de ese grupo no se agregan en automático a la administrative unit, tienes que agregarlos por separado.



1. What type of user account allows an external organization to access your resources?

- A Contributor user account for each member of the team.
 - An administrator account for each member of the team.
 - A guest user account for each member of the external team.
- ✓ Correct. A guest user account restricts users to just the access they need.

2. What kind of group account can you create so you can apply the same permissions to all group members?

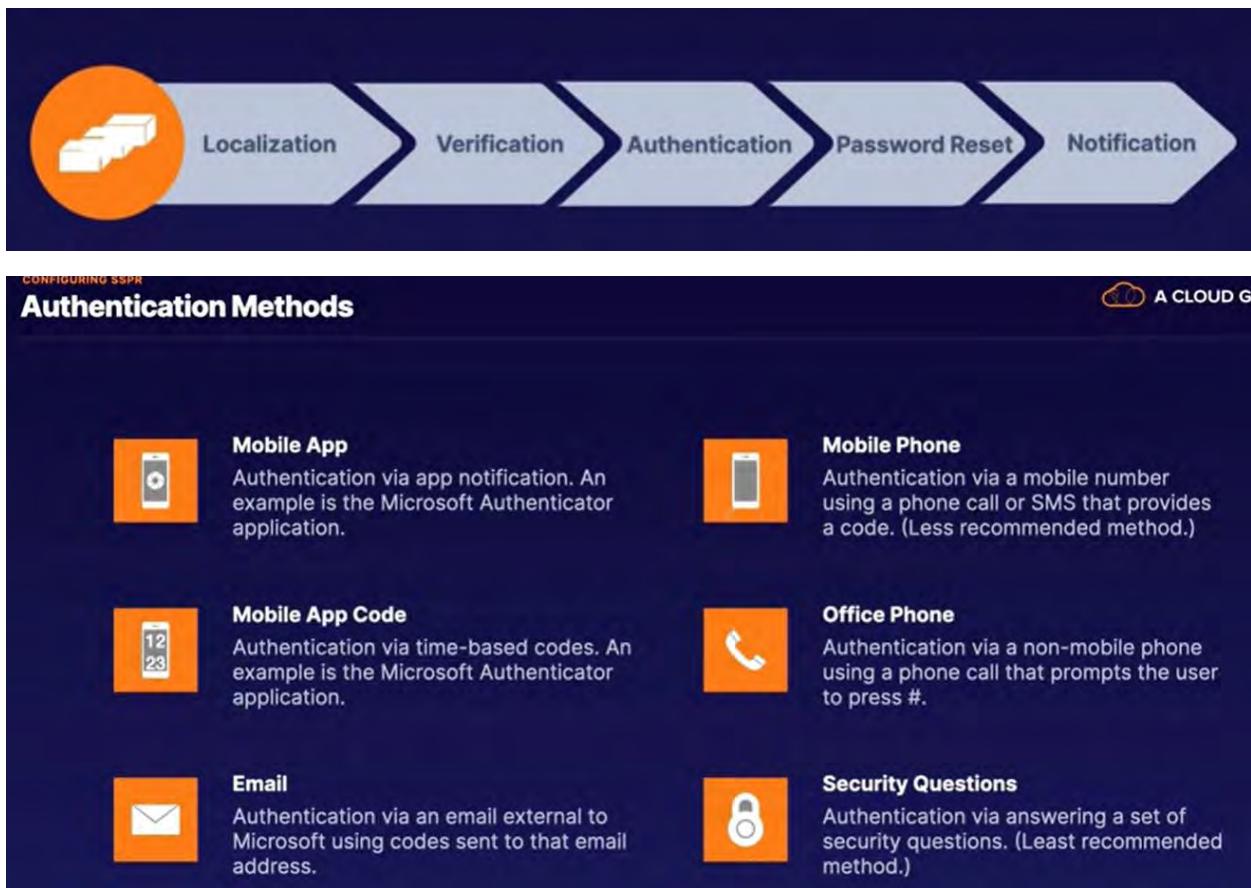
- Security group
- ✓ Correct. You can create a security group for a specific security policy and apply the same permissions to all members of the group.
- Azure AD bulk group
 - Microsoft 365 group

3. Which Azure AD role enables a user to manage all groups in your Teams tenants, and also assign other admin roles?

- Global administrator
- ✓ Correct. The Global Administrator role manages all aspects of Azure AD and Microsoft services that use Azure AD identities. This role can manage groups across tenants and assign other administrator roles.
- Security administrator
 - User administrator

Configuring SSPR (Self Service Password reset)

Permite que cada usuario pueda resetear su contraseña sin ayuda del administrador



Keep In Mind...

Enable and manage SSPR via Azure AD groups.

Required Methods

One or more of the available authentication methods is required for SSPR.



SSPR for Admins

Security questions not available for admins. By default, admins must register for MFA methods.



Required Licenses

Azure AD P1 or P2, Microsoft Apps for Business, or Microsoft 365 licensing is required for SSPR.

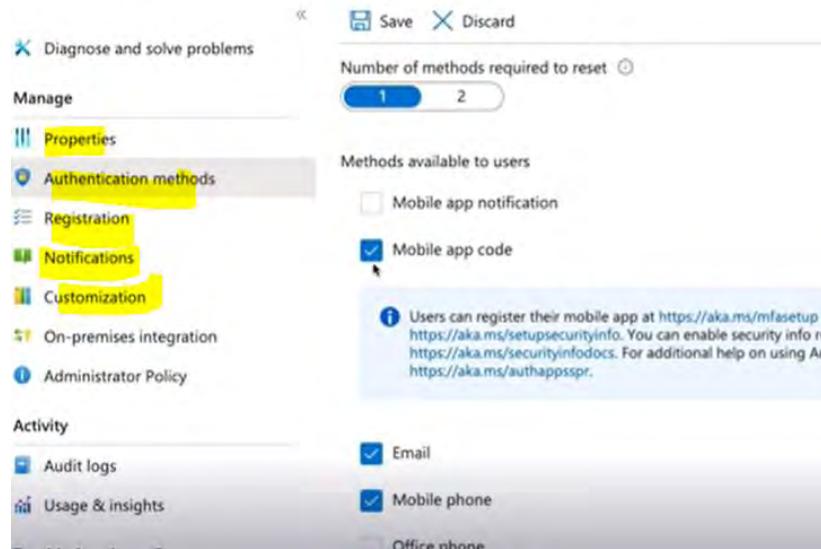


Pasos:

- Ir a Azure AD y crear el SSPR group
- En password reset definimos todo.

Password reset | Authentication methods

Default Directory - Azure Active Directory



The screenshot shows the 'Authentication methods' section of the 'Password reset' configuration. On the left, there's a sidebar with options like 'Properties', 'Authentication methods' (which is selected and highlighted in yellow), 'Registration', 'Notifications', 'Customization', 'On-premises integration', and 'Administrator Policy'. The main area has a 'Save' and 'Discard' button at the top. Below that, it says 'Number of methods required to reset' with a slider set to '1'. Under 'Methods available to users', there are several checkboxes: 'Mobile app notification' (unchecked), 'Mobile app code' (checked), 'Email' (checked), 'Mobile phone' (checked), and 'Office phone' (unchecked). A tooltip for 'Mobile app code' provides instructions on how to register a mobile app at <https://aka.ms/mfasetup> and <https://aka.ms/setupsecurityinfo>.

El factor de autenticación de preguntas no esta disponible para cuentas de admins.

How to Register Devices



Azure AD Registered

Least restrictive option, allowing for Bring Your Own Device (BYOD) with a personal Microsoft or local account. Supports Windows 10, iOS, iPadOS, Android, and macOS.



Azure AD Joined

Device is owned by the organization and accesses AAD through a work account. These identities only exist in the cloud. Supports Windows 10 and Server 2019.



Hybrid Azure AD Joined

Similar to AAD joined, however these device identities exist both on-premises and in the cloud. Supports Windows 7, 8.1, 10, and Server 2008 or later.

NOTE: Requires Azure AD P1 license or Microsoft 365 Business license.

User or Group

Provides fine-grained access to resources based on user identity or group membership.

01

02

Real-Time Risk

Uses Identity Protection to detect risk at sign-in and during a user's session to calculate overall real-time risk.

05



IP Location

Uses an allow list of trusted IP addresses and a deny list of blocked IP addresses to control access to resources.

03

Device

Allows for device type and device state to be evaluated in conditional access policy.

04

Application

Allows control of access to an application on a specific device. Microsoft Cloud App Security can be used to control access to cloud.

Device Identity + Conditional Access =

- Simplified procedure for adding and managing devices
- Improved user experience on devices
- Support for Microsoft Intune
- Single Sign-On (SSO) for any registered or joined devices

Azure AD Join

Soporta Windows 10 y Windows server 2019

Azure AD join works even in hybrid environments, enabling access to both cloud and on-premises apps and resources

Azure AD joined devices are signed in to using an organizational Azure AD account. Access to resources can be controlled based on Azure AD account and [Conditional Access policies](#) applied to the device.

These tools provide a means to enforce organization-required configurations like:

- Requiring storage to be encrypted
- Password complexity
- Software installation
- Software updates

Provisioning Azure AD Join

Manage via Device Settings

Self-Service

Manually configure via Out of Box Experience (OOBE) or from Windows Settings. Technical users only.



Windows Autopilot

Pre-configure OOBE to provide automated device joining and automated MDM enrollment.

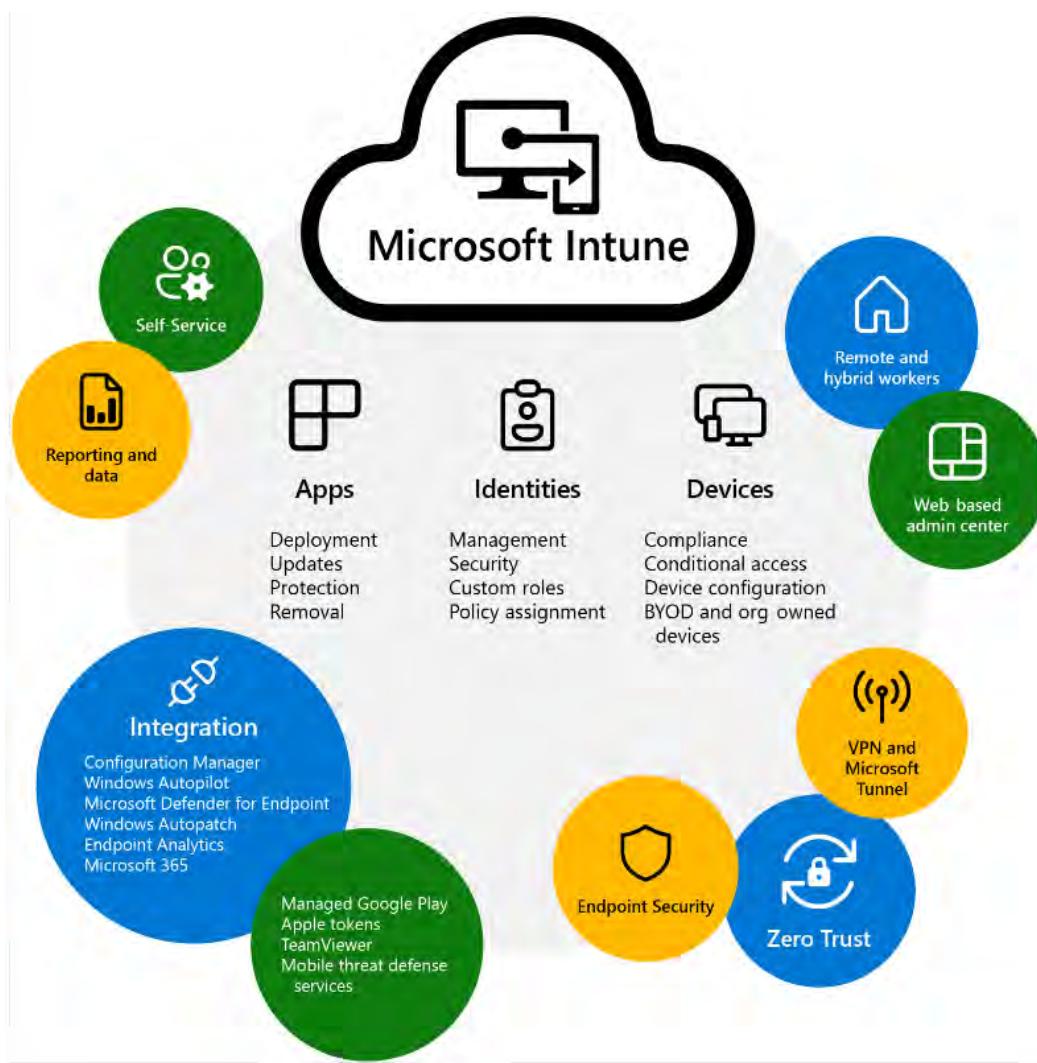


Bulk Enrollment

Use a bulk provisioning tool or package to join a large number of devices.



Microsoft Intune



Understanding Roles in Azure

Three types of roles are available for access management in Azure:

- Classic subscription administrator roles
- Azure role-based access control (RBAC) roles
- Azure Active Directory (Azure AD) administrator roles

Para asignar un rol tienes que definir el rol y luego el alcance de este rol, por ejemplo si no pones en un resource group ese rol también aplicara a los recursos dentro de el.

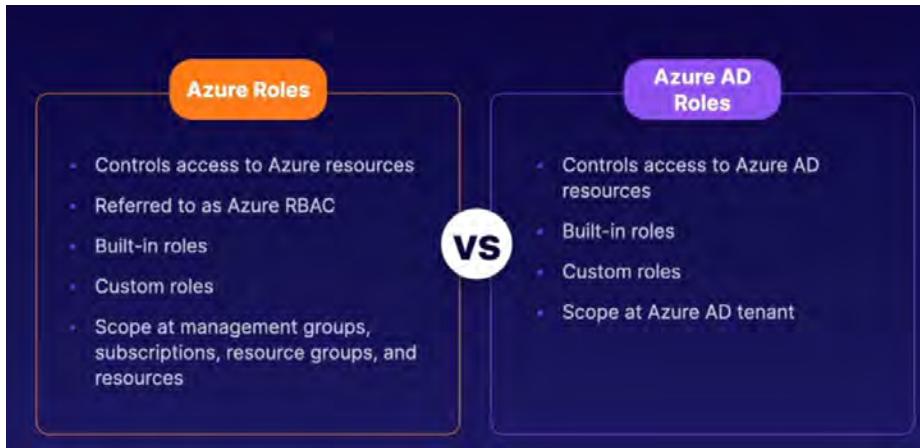
Tipos de roles:

- Owner: Full access to resources and delegates access
- Read only: Can only view resources
- Contributor: Can create and manage resources but not delegate access to other users
- User access administrator: delegate access to resources

Con el Azure AD rol, en vez de dar acceso a los recursos de azure lo hace a los de identity en el azure ad tenant como usuarios y grupos de usuarios. Tipos de roles en azure ad:

- Global admin: Can manage Azure ad resources
- Billing admin: can perform billing tasks
- User admin: can manage users and groups
- Helpdesk Admin: can reset passwords

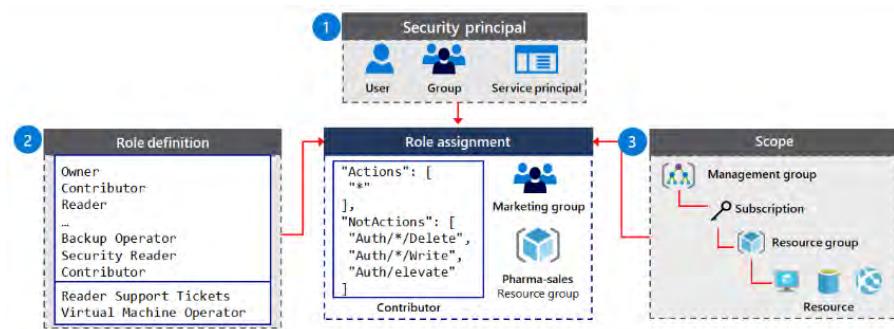
Azure AD Roles	Azure Roles
<ul style="list-style-type: none">♦ Manage access to Azure AD resources♦ Scope is at tenant level♦ Supports custom roles♦ Main roles:<ul style="list-style-type: none">• Global Administrator• User Administrator• Billing Administrator	<ul style="list-style-type: none">♦ Manage access to Azure resources♦ Scope can be at multiple levels♦ Supports custom roles♦ Main roles:<ul style="list-style-type: none">• Owner• Contributor• Reader• User Access Administrator



Things to know about role assignments

Review the following characteristics of role assignments:

- The purpose of a role assignment is to control access.
- The scope limits which permissions defined for a role are available for the assigned requestor.
- Access is revoked by removing a role assignment.
- A resource inherits role assignments from its parent resource.
- The effective permissions for a requestor are a combination of the permissions for the requestor's assigned roles, and the permissions for the roles assigned to the requested resources.



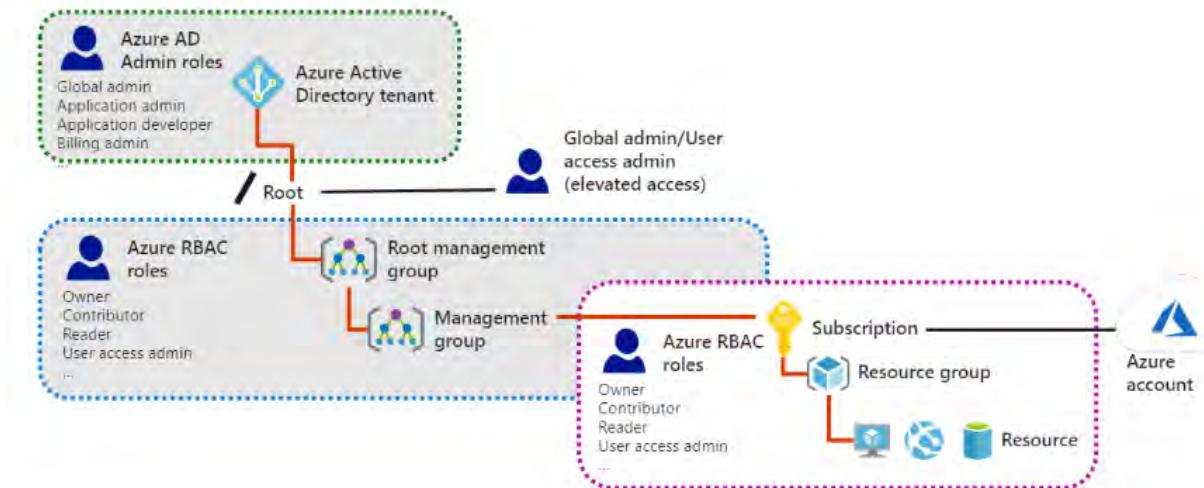
This scenario has the following access management configuration:

- Three security principals are supported: user, group, service principal.
- Six built-in roles are implemented, and two custom roles are defined: Reader Support Tickets and Virtual Machine Operator.
- The built-in Contributor role has two sets of permissions: Actions and NotActions.
- The Contributor role is assigned at different scopes to the Marketing group and Pharma-sales resource group:
 - Users in the Marketing group are granted access to create or manage any Azure resource in the Pharma-sales resource group.
 - Marketing users aren't granted access to resources outside the Pharma-sales resource group, unless they have another role assignment that grants them access to the resource group.

En este ejemplo con el role assignment se le da solo para acceder a los recursos del resource group, pero no se le da para dar acceso al management group de marketing.

Azure RBAC roles	Azure AD admin roles
Access management	Manages access to Azure resources
Scope assignment	Scope can be specified at multiple levels, including management groups, subscriptions, resource groups, and resources
Role definitions	Roles can be defined via the Azure portal, the Azure CLI, Azure PowerShell, Azure Resource Manager templates, and the REST API
	Roles can be defined via the Azure admin portal, Microsoft 365 admin portal, and Microsoft Graph Azure AD PowerShell

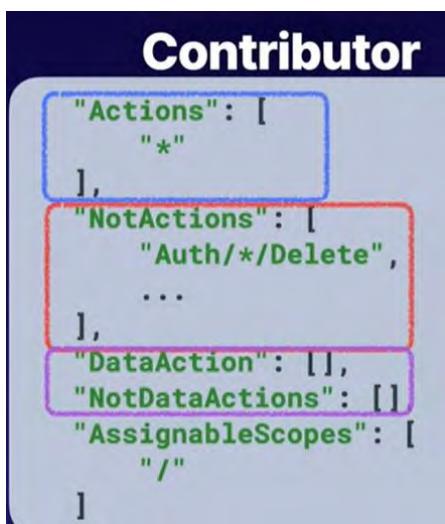
Azure Active Directory (Azure AD) also provides built-in roles to manage resources in Azure AD, including users, groups, and domains. Azure AD offers administrator roles that you can implement for your organization, such as Global admin, Application admin, and Application developer.



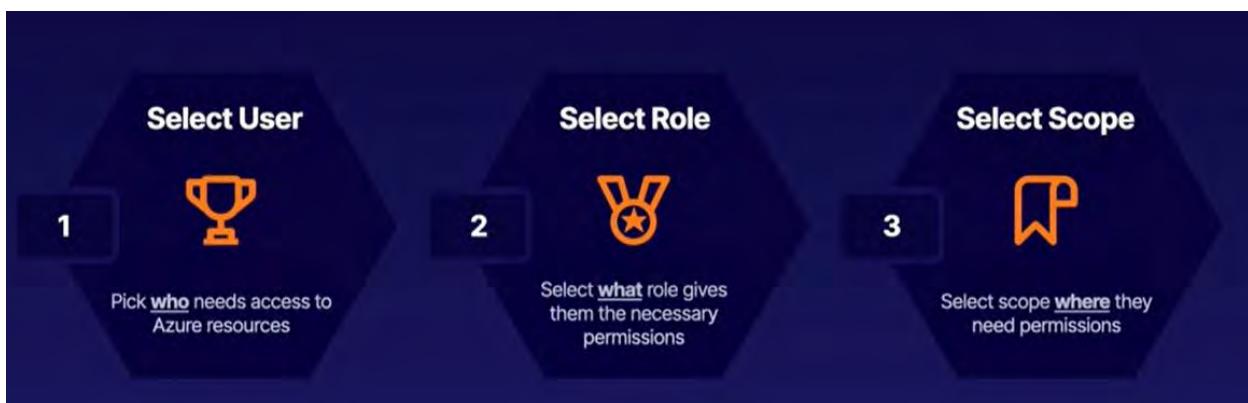
Assigning access to resources



Role definitions:



Si se tienen 2 roles en 2 scopes va a prevalecer el que tenga el scope mas alto



Authorization System

- ✓ Provide identities with access to Azure resources
 - ✓ Roles are a collection of permissions
 - ✓ Scoping hierarchy for role assignments

Creating custom roles

Para crear un custom role es necesario tener user Access admin o owner role en la cuenta

Los custom roes se definen en un json

Creación de un rol:

Azure RBAC provides over 100 pre-defined role definitions. Roles can grant access to data within an object. If a user has *read data* access to a storage account, then they can read the blobs or messages in the storage account.

The following table describes four built-in Azure RBAC role definitions that are considered fundamental.

Fundamental role	Description
Owner	The Owner role has full access to all resources, including the right to delegate access to others. The Service Administrator and Co-Administrators roles are assigned the Owner role at the subscription scope.
Contributor	The Contributor role can create and manage all types of Azure resources. This role can't grant access to others.
Reader	The Reader role can view existing Azure resources.
User Access Administrator	The User Access Administrator role can manage user access to Azure resources.

1. You have three virtual machines (VM1, VM2, VM3) in a resource group. A new admin is hired, and they need to be able to modify settings on VM3. They shouldn't be able to make changes to VM1 or VM2. How can you implement RBAC to minimize administrative overhead?

- Assign the admin to the Contributor role on the resource group.
- Assign the admin to the Contributor role on VM3.
 - ✓ Correct. When you assign the Contributor role to the specific resource, the admin can change the settings on that resource; in this case, VM3.
- Move VM3 to a new resource group, and then assign the admin to the Owner role on VM3.

2. Explain the main differences between Azure roles and Azure Active Directory (Azure AD) roles.

- Azure roles apply to Azure resources. Azure AD roles apply to Azure AD resources such as users, groups, and domains.
 - ✓ Correct. Azure roles are used to manage access to VMs, storage, and other Azure resources. Azure AD roles are used to manage access to Azure AD resources like user accounts and passwords.
- Azure roles can be assigned at the root level.
- Azure AD roles are used to manage access to Azure resources.

3. What's included in a custom Azure role definition?

- Assignment of a custom role
- Actions and DataActions operations scoped to the tenant level
- Operations allowed for Azure resources, and scope of permissions
 - ✓ correct. A custom role definition includes the allowed operations, such as read, write, and delete for Azure resources. The custom role definition also includes the scope of these permissions.

Creación de usuarios y grupos en Azure AD

Adición de cuentas de usuario

Se pueden agregar cuentas de usuario individuales mediante Azure Portal, Azure PowerShell o la CLI de Azure.

Si quiere usar la CLI de Azure, ejecute el cmdlet siguiente:

```
CLI de Azure  
Copiar  
# create a new user  
az ad user create
```

Este comando crea un usuario mediante la CLI de Azure.

Para Azure PowerShell, ejecute el cmdlet siguiente:

```
PowerShell  
Copiar  
# create a new user  
New-AzureADUser
```

Se pueden crear cuentas de usuarios miembros e invitados de forma masiva. En el siguiente ejemplo se muestra cómo invitar a usuarios invitados de forma masiva.

```
PowerShell  
Copiar  
$invitations = import-csv c:\bulkinvite\invitations.csv  
  
$messageInfo = New-Object Microsoft.Open.MSGraph.Model.InvitedUserMessageInfo  
  
$messageInfo.customizedMessageBody = "Hello. You are invited to the Contoso organization."  
  
foreach ($email in $invitations)  
{  
    New-AzureADMSInvitation `  
        -InvitedUserEmailAddress $email.InvitedUserEmailAddress `  
        -InvitedUserDisplayName $email.Name `  
        -InviteRedirectUrl https://myapps.microsoft.com `  
        -InvitedUserMessageInfo $messageInfo `  
        -SendInvitationMessage $true  
}
```

1. Si elimina una cuenta de usuario por error, ¿se puede restaurar?

- Cuando una cuenta de usuario se elimina, es definitivo y no se puede restaurar.
- La cuenta de usuario se puede restaurar, pero solo si se ha creado en los últimos 30 días.
- La cuenta de usuario se puede restaurar, pero solo si se ha eliminado en los últimos 30 días.
 - ✓ Una cuenta de usuario se puede restaurar siempre que se haya eliminado en los últimos 30 días. Vaya a la lista de usuarios eliminados para ver la lista de todos los usuarios eliminados.

2. ¿Qué tipo de cuenta crearía para permitir un acceso fácil a una organización externa?

- Una cuenta de usuario invitado para cada miembro del equipo externo.
 - ✓ Una cuenta de usuario invitado restringe el acceso de los usuarios a únicamente el que necesitan.
- Una cuenta externa para cada miembro del equipo externo.
- Una cuenta de administrador para cada miembro del equipo externo.

Existen diferentes maneras de asignar derechos de acceso:

- **Asignación directa:** asigne a un usuario los derechos de acceso que necesite asignándole directamente un rol que tenga esos derechos de acceso.
- **Asignación de grupos:** asigne a un grupo los derechos de acceso que necesite. Los miembros del grupo heredarán dichos derechos.
- **Asignación basada en reglas:** use reglas para determinar la pertenencia a un grupo en función de las propiedades de usuario o de dispositivo. Para que la pertenencia a un grupo de una cuenta de usuario o de un dispositivo sea válida, el usuario o el dispositivo en cuestión deben cumplir las reglas. Si no las cumplen, la pertenencia al grupo del dispositivo o la cuenta de usuario dejarán de ser válidas. Las reglas pueden ser sencillas. Podemos seleccionar reglas escritas previamente o escribir nuestras propias reglas avanzadas.

With ADFS, you have to create the relying parties, and manage the ADFS infrastructure.

Using ADFS also means the partner you are collaborating with needs a similar SAML type infrastructure so you can federate.

Note that you can also federate your Azure Tenant with a partners Ident Provider as well

<https://learn.microsoft.com/en-us/azure/active-directory/external-identities/direct-federation>

B2B on the other makes all this much simpler and easier to manage. You invite the guests to collaborate allowing for more self-service and allowing you - the resource owner - to focus on the application and not the authentication.



1. What is a role definition in Azure?

- A collection of permissions with a name that is assignable to a user, group, or application
- A role definition in Azure is a collection of permissions with a name that you can assign to a user, group, or application.
- The collection of users, groups, or applications that have permissions to a role
- The binding of a role to a security principal at a specific scope, to grant access

2. Suppose an administrator wants to assign a role to allow a user to create and manage Azure resources but not be able to grant access to others. Which of the following built-in roles would support this?

- Owner
- Contributor
- A contributor can create and manage all types of Azure resources, but they can't grant access to other users.
- Reader
- User Access Administrator

3. What is the inheritance order for scope in Azure?

- Management group, Resource group, Subscription, Resource
- Management group, Subscription, Resource group, Resource
- The inheritance order for scope is Management group, Subscription, Resource group, Resource. For example, if you assigned a Contributor role to a group at the Subscription scope level, it will be inherited by all Resource groups and Resources.
- Subscription, Management group, Resource group, Resource
- Subscription, Resource group, Management group, Resource

1. Suppose a team member can't view resources in a resource group. Where would the administrator go to check the team member's access?

- Check the team member's permissions by going to their Azure profile > My permissions.
- Go to the resource group and select Access control (IAM) > Check Access.
✓ Find the list of role assignments on the resource group.
- Go to one of the resources in the resource group and select Role assignments.

2. Suppose an administrator in another department needs access to a virtual machine managed by your department. What's the best way to grant them access to just that resource?

- At the resource scope, create a role for them with the appropriate access.
- At the resource group scope, assign the role with the appropriate access.
- At the resource scope, assign the role with the appropriate access.
✓ For this scenario, at the virtual machine scope, assign one of the built-in roles that grants the appropriate access for the administrator.

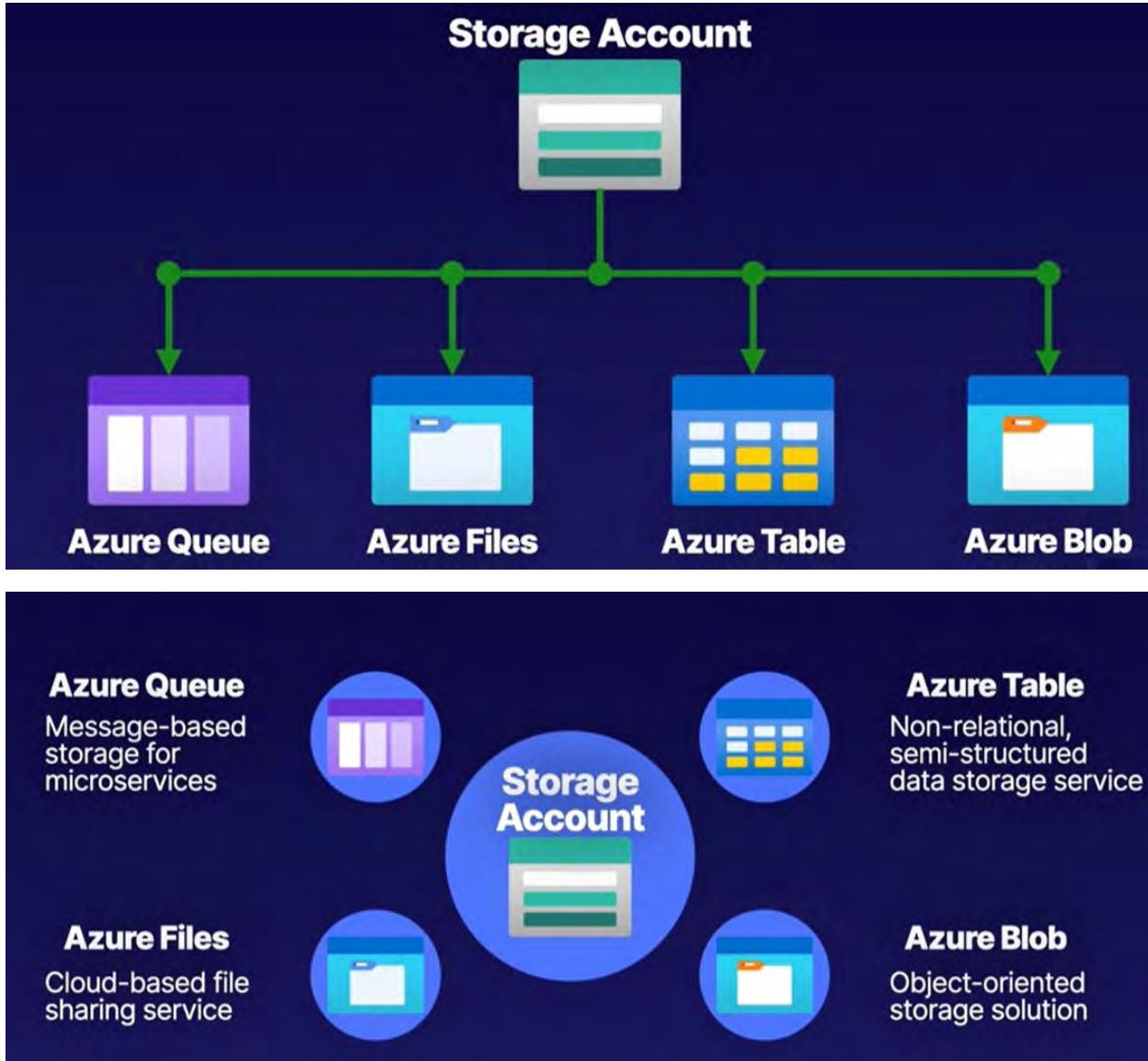
3. Suppose a developer needs full access to a resource group. If you are following least-privilege best practices, what scope should you specify?

- Resource
- Resource group
✓ Following least-privilege best practices, you grant only the access the user needs to do their job. In this case, you should set the scope to the resource group.
- Subscription

4. Suppose an administrator needs to generate a report of the role assignments for the last week. Where in the Azure portal would they generate that report?

- Search for Activity log and filter on the Create role assignment (roleAssignments) operation.
✓ In the Activity log, filter on the Operation name field to find role assignments.
- At the appropriate scope, go to Access control (IAM) > Download role assignments.
- At the appropriate scope, go to Access control (IAM) > Role assignments.

STORAGE ACCOUNTS



Implement Azure Storage

✓ 100 XP

3 minutes

Azure Storage is Microsoft's cloud storage solution for modern data storage scenarios. Azure Storage offers a massively scalable object store for data objects. It provides a file system service for the cloud, a messaging store for reliable messaging, and a [NoSQL store](#).

You can think of Azure Storage as supporting three categories of data: structured data, unstructured data, and virtual machine data. Review the following categories and think about which types of storage are used in your organization.

Category	Description	Storage examples
Virtual machine data	Virtual machine data storage includes disks and files. Disks are persistent block storage for Azure IaaS virtual machines. Files are fully managed file shares in the cloud.	Storage for virtual machine data is provided through Azure managed disks. Data disks are used by virtual machines to store data like database files, website static content, or custom application code. The number of data disks you can add depends on the virtual machine size. Each data disk has a maximum capacity of 32,767 GB. → TB
Unstructured data	Unstructured data is the least organized. It can be a mix of information that's stored together, but the data doesn't have a clear relationship. The format of unstructured data is referred to as <i>non-relational</i> .	Unstructured data can be stored by using Azure Blob Storage and Azure Data Lake Storage. Blob Storage is a highly scalable, REST-based cloud object store. Azure Data Lake Storage is the Hadoop Distributed File System (HDFS) as a service.
Structured data	Structured data is stored in a relational format that has a shared schema. Structured data is often contained in a database table with rows, columns, and keys. Tables are an autoscaling NoSQL store.	Structured data can be stored by using Azure Table Storage, Azure Cosmos DB, and Azure SQL Database. Azure Cosmos DB is a globally distributed database service. Azure SQL Database is a fully managed database-as-a-service built on SQL.

Blob storage podemos guardar virtual hdd, imágenes y videos

Resource group>storage account>(azure Queue, azure files, azure table, azure blob)

Components of storage accounts:



Access tier es el que pondremos por default a nuestros recursos.

Tipos de redundancia al crear un storage account:

Locally-redundant storage (LRS):

Lowest-cost option with basic protection against server rack and drive failures. Recommended for non-critical scenarios.

Geo-redundant storage (GRS):

Intermediate option with failover capabilities in a secondary region. Recommended for backup scenarios.

Zone-redundant storage (ZRS):

Intermediate option with protection against datacenter-level failures. Recommended for high availability scenarios.

Geo-zone-redundant storage (GZRS):

Optimal data protection solution that includes the offerings of both GRS and ZRS. Recommended for critical data scenarios.

Locally redundant storage

Locally redundant storage is the **lowest-cost replication option** and offers the least durability compared to other strategies. If a data center-level disaster occurs, such as fire or flooding, all replicas might be lost or unrecoverable. Despite its limitations, LRS can be appropriate in several scenarios:

- Your application stores data that can be easily reconstructed if data loss occurs.
- Your data is constantly changing like in a live feed, and storing the data isn't essential.
- Your application is restricted to replicating data only within a country/region due to data governance requirements.

Zone redundant storage

Zone redundant storage synchronously replicates your data across three storage clusters in a single region. Each storage cluster is physically separated from the others and resides in its own availability zone. Each availability zone, and the ZRS cluster within it, is autonomous, and has separate utilities and networking capabilities. Storing your data in a ZRS account ensures you can access and manage your data if a zone becomes unavailable. ZRS provides excellent performance and low latency.

- ZRS isn't currently available in all regions.
- Changing to ZRS from another data replication option requires the physical data movement from a single storage stamp to multiple stamps within a region.

Geo-redundant storage

Geo-redundant storage replicates your data to a secondary region (hundreds of miles away from the primary location of the source data). GRS provides a higher level of durability even during a regional outage. GRS is designed to provide at least **99.999999999999% (16 9s) durability**. When your storage account has GRS enabled, your data is durable even when there's a complete regional outage or a disaster where the primary region isn't recoverable.

If you implement GRS, you have two related options to choose from:

- GRS replicates your data to another data center in a secondary region. The data is available to be read only if Microsoft initiates a failover from the primary to secondary region.
- Read-access geo-redundant storage (RA-GRS) is based on GRS. RA-GRS replicates your data to another data center in a secondary region, and also provides you with the option to read from the secondary region. With RA-GRS, you can read from the secondary region regardless of whether Microsoft initiates a failover from the primary to the secondary.

For a storage account with GRS or RA-GRS enabled, all data is first replicated with locally redundant storage. An update is first committed to the primary location and replicated by using LRS. The update is then replicated asynchronously to the secondary region by using GRS. When data is written to the secondary location, it's also replicated within that location by using LRS. Both the primary and secondary regions manage replicas across separate fault domains and upgrade domains within a storage scale unit. The storage scale unit is the basic replication unit within the datacenter. Replication at this level is provided by LRS.

Geo-zone redundant storage

Geo-zone-redundant storage combines the high availability of zone-redundant storage with protection from regional outages as provided by geo-redundant storage. Data in a GZRS storage account is replicated across three Azure availability zones in the primary region, and also replicated to a secondary geographic region for protection from regional disasters. Each Azure region is paired with another region within the same geography, together making a regional pair.

With a GZRS storage account, you can continue to read and write data if an availability zone becomes unavailable or is unrecoverable. Additionally, your data is also durable during a complete regional outage or during a disaster in which the primary region isn't recoverable. GZRS is designed to provide at least 99.999999999999% (16 9's) durability of objects over a given year. GZRS also offers the same scalability targets as LRS, ZRS, GRS, or RA-GRS. You can optionally enable read access to data in the secondary region with read-access geo-zone-redundant storage (RA-GZRS).

Things to consider when choosing replication strategies

Let's examine the scope of durability and availability for the different replication strategies. The following table describes several key factors during the replication process, including node unavailability within a data center, and whether the entire data center (zonal or non-zonal) becomes unavailable. The table identifies read access to data in a remote, geo-replicated region during region-wide unavailability, and the supported Azure storage account types.

Node in data center unavailable	Entire data center unavailable	Region-wide outage	Read access during region-wide outage	Supported storage accounts
- LRS	- ZRS	- GRS	- RA-GRS	- LRS: GPv1, GPv2, Blob
- ZRS	- GRS	- RA-GRS	- RA-GZRS	- ZRS: GPv2
- GRS	- RA-GRS	- GZRS	-	- GRS: GPv1, GPv2, Blob
- RA-GRS	- GZRS	- RA-GZRS	-	- RA-GRS: GPv1, GPv2, Blob
- GZRS	- RA-GZRS	-	-	- GZRS: GPv2
- RA-GZRS	-	-	-	- RA-GZRS: GPv2

Grs se replica en otra región y gtrs se replita en otra región y también en availabilities zones de la región principal

🔗 Durability and availability parameters

The following table describes key parameters for each redundancy option:

Parameter	LRS	ZRS	GRS/RA-GRS	GZRS/RA-GZRS
Percent durability of objects over a given year	at least 99.999999999% (11 9's)	at least 99.999999999% (12 9's)	at least 99.9999999999999% (16 9's)	at least 99.9999999999999% (16 9's)
Availability for read requests	At least 99.9% (99% for Cool or Archive access tiers)	At least 99.9% (99% for Cool or Archive access tiers)	At least 99.9% (99% for Cool or Archive access tiers) for GRS At least 99.99% (99.9% for Cool or Archive access tiers) for RA-GRS	At least 99.9% (99% for Cool or Archive access tiers) for GZRS At least 99.99% (99.9% for Cool or Archive access tiers) for RA-GZRS
Availability for write requests	At least 99.9% (99% for Cool or Archive access tiers)	At least 99.9% (99% for Cool or Archive access tiers)	At least 99.9% (99% for Cool or Archive access tiers)	At least 99.9% (99% for Cool or Archive access tiers)
Number of copies of data maintained on separate nodes	Three copies within a single region	Three copies across separate availability zones within a single region	Six copies total, including three in the primary region and three in the secondary region	Six copies total, including three across separate availability zones in the primary region and three locally redundant copies in the secondary region

Durability and availability by outage scenario

The following table indicates whether your data is durable and available in a given scenario, depending on which type of redundancy is in effect for your storage account:

Outage scenario	LRS	ZRS	GRS/RA-GRS	GZRS/RA-GZRS
A node within a data center becomes unavailable	Yes	Yes	Yes	Yes
An entire data center (zonal or non-zonal) becomes unavailable	No	Yes	Yes ¹	Yes
A region-wide outage occurs in the primary region	No	No	Yes ¹	Yes ¹
Read access to the secondary region is available if the primary region becomes unavailable	No	No	Yes (with RA-GRS)	Yes (with RA-GZRS)

¹ Account failover is required to restore write availability if the primary region becomes unavailable. For more information, see [Failover and failback](#).

Supported Azure Storage services

The following table shows which redundancy options are supported by each Azure Storage service.

LRS	ZRS	GRS	RA-GRS	GZRS	RA-GZRS
Blob storage (including Data Lake Storage)					
Queue storage					
Table storage					
Azure Files ^{1,2}	Azure Files ^{1,2}	Azure Files ¹		Azure Files ¹	
Azure managed disks	Azure managed disks ³				
Page blobs					

El nombre del storage account debe ser único en todo azure.

Se crean 3 copias localmente en el de redundancia local.

Acess tiers en storage accounts:

Access tier ⓘ

Hot: Frequently accessed data and day-to-day usage scenarios

Cool: Infrequently accessed data and backup scenarios

Account Type	General Purpose v1	Legacy for blobs, files, queues, and tables
	General Purpose v2	Recommended for blobs, files, queues, and tables
Performance Tier	Blob Storage	Legacy blob-specific accounts
	Standard	Default storage performance tier
	Premium	High-performance storage tier
Replication	Locally Redundant Storage (LRS)	3 copies in a physical location within a region
	Zone-Redundant Storage (ZRS)	3 copies across zones within a region
	Geo-Redundant Storage (GRS)	GRS in a primary and secondary region
	Geo-Zone Redundant Storage (GZRS)	ZRS in a primary region and LRS in a secondary region
Access Tier	Hot	Frequently accessed data
	Cold	Infrequently accessed data
	Archive	Backup data rarely accessed

Storage account	Supported services	Recommended usage
Standard general-purpose v2	Blob Storage (including Data Lake Storage), Queue Storage, Table Storage, and Azure Files	Standard storage account for most scenarios, including blobs, file shares, queues, tables, and disks (page blobs).
Premium block blobs	Blob Storage (including Data Lake Storage)	Premium storage account for block blobs and append blobs. Recommended for applications with high transaction rates. Use Premium block blobs if you work with smaller objects or require consistently low storage latency. This storage is designed to scale with your applications.
Premium file shares	Azure Files	Premium storage account for file shares only. Recommended for enterprise or high-performance scale applications. Use Premium file shares if you require support for both Server Message Block (SMB) and NFS file shares.
Premium page blobs	Page blobs only	Premium high-performance storage account for page blobs only. Page blobs are ideal for storing index-based and sparse data structures, such as operating systems, data disks for virtual machines, and databases.

① Note

All storage account types are encrypted by using Storage Service Encryption (SSE) for data at rest.

Storage account tiers

General purpose Azure storage accounts have two tiers: Standard and Premium.

- Standard storage accounts are backed by magnetic hard disk drives (HDD). A standard storage account provides the lowest cost per GB. You can use Standard tier storage for applications that require bulk storage or where data is infrequently accessed.
- Premium storage accounts are backed by solid-state drives (SSD) and offer consistent low-latency performance. You can use Premium tier storage for Azure virtual machine disks with I/O-intensive applications like databases.

① Note

You can't convert a Standard tier storage account to a Premium tier storage account or vice versa. You must create a new storage account with the desired type and copy data, if applicable, to a new storage account.

Things to consider when using Azure Storage

As you think about your configuration plan for Azure Storage, consider these prominent features.

- Consider durability and availability. Azure Storage is durable and highly available. Redundancy ensures your data is safe during transient hardware failures. You replicate data across datacenters or geographical regions for protection from local catastrophe or natural disaster. Data that's replicated remains highly available during an unexpected outage.
- Consider secure access. All data written to Azure Storage is encrypted by the service. Azure Storage provides you with fine-grained control over who has access to your data.
- Consider scalability. Azure Storage is designed to be massively scalable to meet the data storage and performance needs of modern applications.
- Consider manageability. Microsoft Azure handles hardware maintenance, updates, and critical issues for you.
- Consider data accessibility. Data in Azure Storage is accessible from anywhere in the world over HTTP or HTTPS. Microsoft provides SDKs for Azure Storage in various languages. You can use .NET, Java, Node.js, Python, PHP, Ruby, Go, and the REST API. Azure Storage supports scripting in Azure PowerShell or the Azure CLI. The Azure portal and Azure Storage Explorer offer easy visual solutions for working with your data.

Service	Default endpoint
Container service	// mystorageaccount.blob.core.windows.net
Table service	// mystorageaccount.table.core.windows.net
Queue service	// mystorageaccount.queue.core.windows.net
File service	// mystorageaccount.file.core.windows.net

Configure custom domains

You can configure a custom domain to access blob data in your Azure storage account. As we reviewed, the default endpoint for Azure Blob Storage is `<storage-account-name>.blob.core.windows.net`. You can also use the web endpoint that's generated as a part of the static websites feature. If you map a custom domain and subdomain, such as `www.contoso.com`, to the blob or web endpoint for your storage account, your users can use that domain to access blob data in your storage account.

ⓘ Note

Azure Storage doesn't currently provide native support for HTTPS with custom domains. You can implement an Azure Content Delivery Network (CDN) to access blobs by using custom domains over HTTPS.

There are two ways to configure a custom domain: direct mapping and intermediary domain mapping.

- Direct mapping lets you enable a custom domain for a subdomain to an Azure storage account. For this approach, you create a `CNAME` record that points from the subdomain to the Azure storage account.

The following example shows how a subdomain is mapped to an Azure storage account to create a `CNAME` record in the domain name system (DNS):

- Subdomain: `blobs.contoso.com`
- Azure storage account: `<storage account>.blob.core.windows.net`
- Direct `CNAME` record: `contosoblobs.blob.core.windows.net`

- Intermediary domain mapping is applied to a domain that's already in use within Azure. This approach might result in minor downtime while the domain is being mapped. To avoid downtime, you can use the `asverify` intermediary domain to validate the domain. By prepending the `asverify` keyword to your own subdomain, you permit Azure to recognize your custom domain without modifying the DNS record for the domain. After you modify the DNS record for the domain, your domain is mapped to the blob endpoint with no downtime.

The following example shows how a domain in use is mapped to an Azure storage account in the DNS with the `asverify` intermediary domain:

- `CNAME` record: `asverify .blobs.contoso.com`
- Intermediate `CNAME` record: `asverify .contosoblobs.blob.core.windows.net`

Things to know about configuring service endpoints

Here are some points to consider about configuring service access settings:

- The Firewalls and virtual networks settings restrict access to your storage account from specific subnets on virtual networks or public IPs.
- You can configure the service to allow access to one or more public IP ranges.
- Subnets and virtual networks must exist in the same Azure region or region pair as your storage account.

Answer the following questions

Choose the best response for each of the questions below. Then select Check your answers.

1. Which storage solution replicates data to a secondary region, and maintains six copies of the data?

Locally redundant storage

Read-access geo-redundant storage

✓ Correct. Read-access geo-redundant storage is the default replication option. Geo-redundant storage (GRS) copies the data synchronously three times within a single physical location in the primary region by using LRS. The data is then copied asynchronously to a single physical location in the secondary region.

Zone-redundant storage

2. The admin team needs to know the requirements for storage account names. To what extent does a storage account name need to be unique?

The name must be unique within the containing resource group.

The name must be unique within the organization's subscription.

The name must be globally unique.

✓ Correct. The storage account name is used as part of the URI for API access, so it must be globally unique.

3. What's the best storage account solution to support the requirements of the manufacturing division?

Locally redundant storage

✓ Correct. Locally redundant storage is the best choice. It's the lowest cost solution, the data is being continuously created, and data loss isn't an issue.

Geo-redundant storage

Zone-redundant storage

Conceptualizing Azure Blob Storage

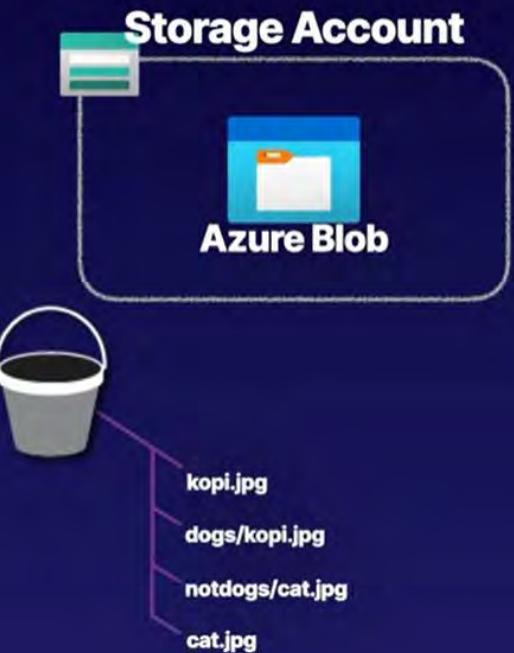
Blob Storage

Azure Blob is a sub-service/sub-resource of Azure Storage (storage accounts).

Blob storage is our object-based storage. Easily accessible from HTTP/REST.

Store items such as:

- Image/Video files
- Text files
- Log files
- VHD (Virtual Hard Disks) files



Blob Service

Blob service is a sub-service for storage accounts.



Blob Container

The container where we store our blobs.

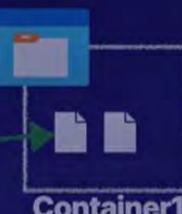


Blobs

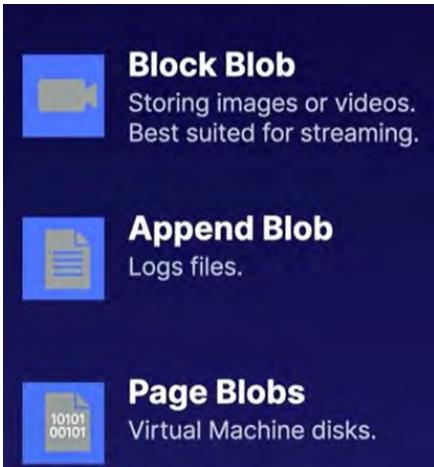
The data we are storing in our containers.



Storage Account



Tipos de blobs:



Things to know about blob types

Let's take a closer look at the characteristics of blob types.

- **Block blobs.** A block blob consists of blocks of data that are assembled to make a blob. Most Blob Storage scenarios use block blobs. Block blobs are ideal for storing text and binary data in the cloud, like files, images, and videos.
- **Append blobs.** An append blob is similar to a block blob because the append blob also consists of blocks of data. The blocks of data in an append blob are optimized for append operations. Append blobs are useful for logging scenarios, where the amount of data can increase as the logging operation continues.
- **Page blobs.** A page blob can be up to 8 TB in size. Page blobs are more efficient for frequent read/write operations. Azure Virtual Machines uses page blobs for operating system disks and data disks.
- The block blob type is the default type for a new blob. When you're creating a new blob, if you don't choose a specific type, the new blob is created as a block blob.
- After you create a blob, you can't change its type.



Si hay blobs o containers con el signo \$ significa que fueron creados por el sistema automáticamente.

Azure Blob Storage (containers)

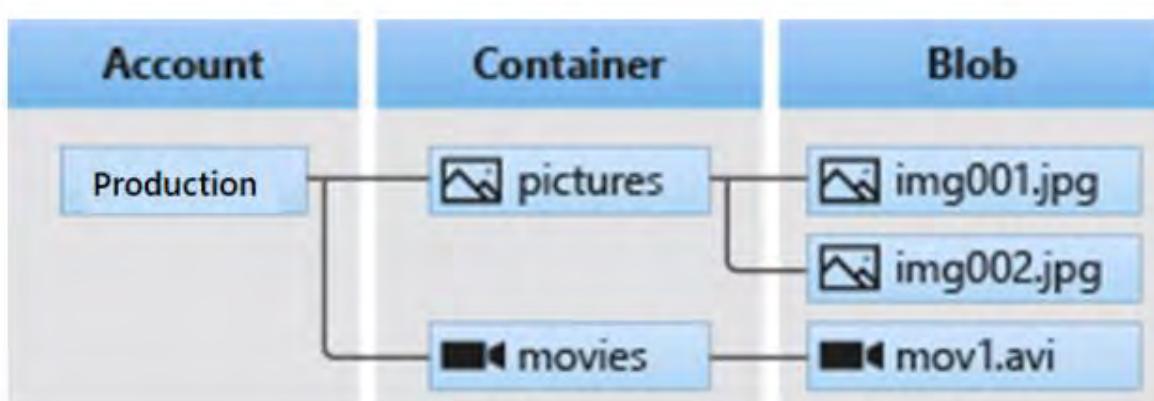
Azure Blob Storage is Microsoft's object storage solution for the cloud. Blob Storage is optimized for storing massive amounts of unstructured or *non-relational* data, such as text or binary data. Blob Storage is ideal for:

- 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.

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, the 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.

ⓘ Note

You can access data from Azure Blob Storage by using the NFS protocol.



Things to consider when implementing Azure Blob Storage

There are many common uses for Blob Storage. Consider the following scenarios and think about your own data needs:

- Consider browser uploads. Use Blob Storage to serve images or documents directly to a browser.
- Consider distributed access. Blob Storage can store files for distributed access, such as during an installation process.
- Consider streaming data. Stream video and audio by using Blob Storage.
- Consider archiving and recovery. Blob Storage is a great solution for storing data for backup and restore, disaster recovery, and archiving.
- Consider application access. You can store data in Blob Storage for analysis by an on-premises or Azure-hosted service.

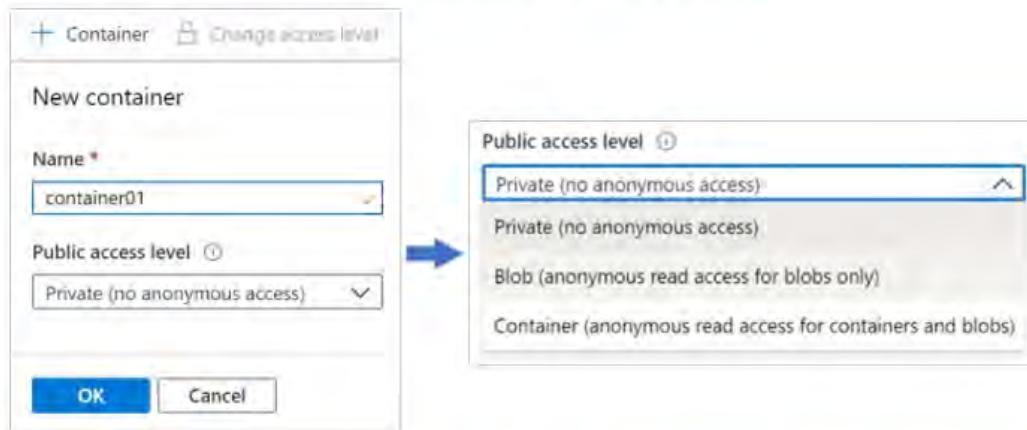
Things to know about containers and blobs

Let's look at the configuration characteristics of containers and blobs.

- All blobs must be in a container.
- A container can store an unlimited number of blobs.
- An Azure storage account can contain an unlimited number of containers.
- You can create the container in the Azure portal.
- You upload blobs into a container.

Configure a container

In the Azure portal, you configure two settings to create a container for an Azure storage account. As you review these details, consider how you might organize containers in your storage account.



- Name: Enter a name for your container. The name must be unique within the Azure storage account.
 - The name can contain only lowercase letters, numbers, and hyphens.
 - The name must begin with a letter or a number.
 - The minimum length for the name is three characters.
 - The maximum length for the name is 63 characters.
- Public access level: The access level specifies whether the container and its blobs can be accessed publicly. By default, container data is private and visible only to the account owner. There are three access level choices:
 - Private: (Default) Prohibit anonymous access to the container and blobs.
 - Blob: Allow anonymous public read access for the blobs only.
 - Container: Allow anonymous public read and list access to the entire container, including the blobs.

Let's examine characteristics of the blob access tiers.

Hot tier

The Hot tier is optimized for frequent reads and writes of objects in the Azure storage account. A good usage case is data that is actively being processed. By default, new storage accounts are created in the Hot tier. This tier has the lowest access costs, but higher storage costs than the Cool and Archive tiers.

Cool tier

The Cool tier is optimized for storing large amounts of data that's infrequently accessed. This tier is intended for data that remains in the Cool tier for at least 30 days. A usage case for the Cool tier is short-term backup and disaster recovery datasets and older media content. This content shouldn't be viewed frequently, but it needs to be immediately available. Storing data in the Cool tier is more cost-effective. Accessing data in the Cool tier can be more expensive than accessing data in the Hot tier.

Archive tier

The Archive tier is an offline tier that's optimized for data that can tolerate several hours of retrieval latency. Data must remain in the Archive tier for at least 180 days or be subject to an early deletion charge. Data for the Archive tier includes secondary backups, original raw data, and legally required compliance information. This tier is the most cost-effective option for storing data. Accessing data is more expensive in the Archive tier than accessing data in the other tiers.

Compare	Hot tier	Cool tier	Archive tier
Availability	99.9%	99%	Offline
Availability (RA-GRS reads)	99.99%	99.9%	Offline
Latency (time to first byte)	milliseconds	milliseconds	hours
Minimum storage duration	N/A	30 days	180 days
Usage costs	Higher storage costs, Lower access & transaction costs	Lower storage costs, Higher access & transaction costs	Lowest storage costs, Highest access & transaction costs

A common approach for uploading blobs to your Azure storage account is to use [Azure Storage Explorer](#). Many other tools are also available. Review the following options and consider which tools would suit your configuration needs.

Upload tool	Description
AzCopy	An easy-to-use command-line tool for Windows and Linux. You can copy data to and from Blob Storage, across containers, and across storage accounts.
Azure Data Box Disk	A service for transferring on-premises data to Blob Storage when large datasets or network constraints make uploading data over the wire unrealistic. You can use Azure Data Box Disk to request solid-state disks (SSDs) from Microsoft. You can copy your data to those disks and ship them back to Microsoft to be uploaded into Blob Storage.
Azure Import/Export	A service that helps you export large amounts of data from your storage account to hard drives that you provide and that Microsoft then ships back to you with your data.

Things to know about pricing for Blob Storage

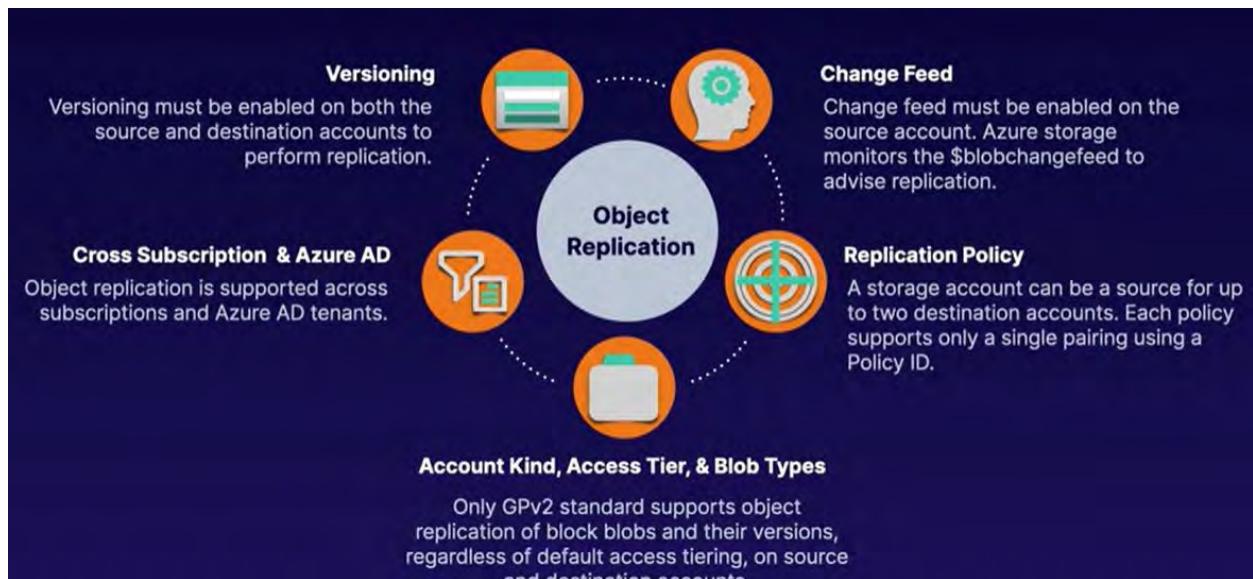
Review the following billing considerations for an Azure storage account and Blob Storage.

- **Performance tiers.** The Blob Storage tier determines the amount of data stored and the cost for storing that data. As the performance tier gets cooler, the per-gigabyte cost decreases.
- **Data access costs.** Data access charges increase as the tier gets cooler. For data in the Cool and Archive tiers, you're billed a per-gigabyte data access charge for reads.
- **Transaction costs.** There's a per-transaction charge for all tiers. The charge increases as the tier gets cooler.
- **Geo-replication data transfer costs.** This charge only applies to accounts that have geo-replication configured, including GRS and RA-GRS. Geo-replication data transfer incurs a per-gigabyte charge.
- **Outbound data transfer costs.** Outbound data transfers (data that's transferred out of an Azure region) incur billing for bandwidth usage on a per-gigabyte basis. This billing is consistent with general-purpose Azure storage accounts.
- **Changes to the storage tier.** If you change the account storage tier from Cool to Hot, you incur a charge equal to reading all the data existing in the storage account. Changing the account storage tier from Hot to Cool incurs a charge equal to writing all the data into the Cool tier (GPv2 accounts only).

Configuring blob object replication

Object replication: replicates your blobs in 2 different regions or zones

Benefits:



\$blobchangefeed: se crea en la storage account y checa cuando hay algun cambio en el blob y avisa para replicar el objeto del src al destino

Hay source account y destination account, en la de destination es a donde se va a replicar

Se pueden tener hasta 2 destination accounts



Versioning

Versioning must be enabled on both the source and destination accounts to perform replication.



Cross Subscription & Azure AD

Object replication is supported across subscriptions and Azure AD tenants.



Change Feed

Change feed must be enabled on the source account. Azure storage monitors the \$blobchangefeed to advise replication.



Replication Policy

A storage account can be a source for up to two destination accounts. Each policy supports only a single pairing using a Policy



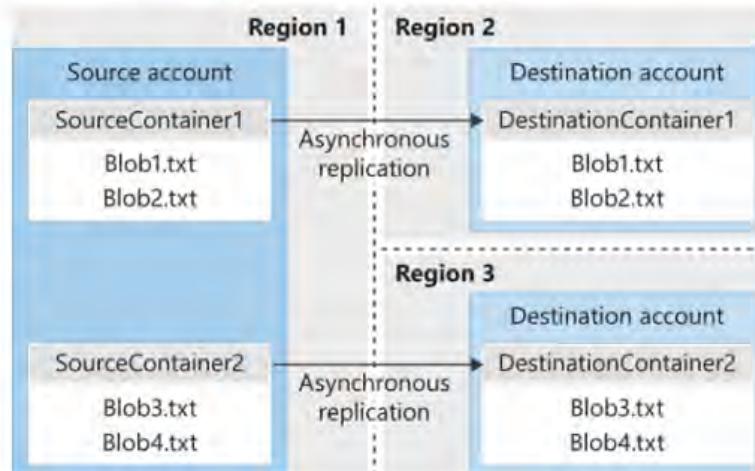
Account Kind, Access Tier, & Blob Types

Only GPv2 standard supports object replication of block blobs and their versions, regardless of default access tiering, on source and destination accounts.

Object replication copies blobs in a container asynchronously according to policy rules that you configure. During the replication process, the following contents are copied from the source container to the destination container:

- The blob contents
- The blob metadata and properties
- Any versions of data associated with the blob

The following illustration shows an example of asynchronous replication of blob containers between regions.



Things to know about blob object replication

There are several considerations to keep in mind when planning your configuration for blob object replication.

- Object replication requires that blob versioning is enabled on both the source and destination accounts.
- Object replication doesn't support blob snapshots. Any snapshots on a blob in the source account aren't replicated to the destination account.
- Object replication is supported when the source and destination accounts are in the Hot or Cool tier. The source and destination accounts can be in different tiers.
- When you configure object replication, you create a replication policy that specifies the source Azure storage account and the destination storage account.
- A replication policy includes one or more rules that specify a source container and a destination container. The policy identifies the blobs in the source container to replicate.

Things to consider when configuring blob object replication

There are many benefits to using blob object replication. Consider the following scenarios and think about how replication can be a part of your Blob Storage strategy.

- Consider latency reductions. Minimize latency with blob object replication. You can reduce latency for read requests by enabling clients to consume data from a region that's in closer physical proximity.
- Consider efficiency for compute workloads. Improve efficiency for compute workloads by using blob object replication. With object replication, compute workloads can process the same sets of blobs in different regions.
- Consider data distribution. Optimize your configuration for data distribution. You can process or analyze data in a single location and then replicate only the results to other regions.
- Consider costs benefits. Manage your configuration and optimize your storage policies to achieve cost benefits. After your data is replicated, you can reduce costs by moving the data to the Archive tier by using lifecycle management policies.

1. What statement best describes Azure Blob Storage access tiers?

- The cool access tier is for frequent access of objects in the storage account.
- The hot access tier is for storing large amounts of data that's infrequently accessed.
- The administrator can switch between hot and cool performance tiers at any time.

✓ Correct. The administrator can switch between hot and cool performance tiers at any time.

2. Which of the following changes between access tiers happens immediately?

- Hot tier to cool tier
- Archive tier to cool tier
- Archive tier to hot tier

✓ Correct. Changes between the hot and cool tiers, and to the archive tier, happen immediately

- Blob object replication doesn't require versioning to be enabled.
- Blob object replication doesn't support blob snapshots.
- Blob object replication is supported in the archive tier.

✓ Correct. Any snapshots on a blob in the source account aren't replicated to the destination account.

Configuring blob lifecycle management

Lifecycle management: a feature of the blob service that enables automation to manage the lifecycle of blobs, by moving blobs between access tiers, to optimize storage costs.

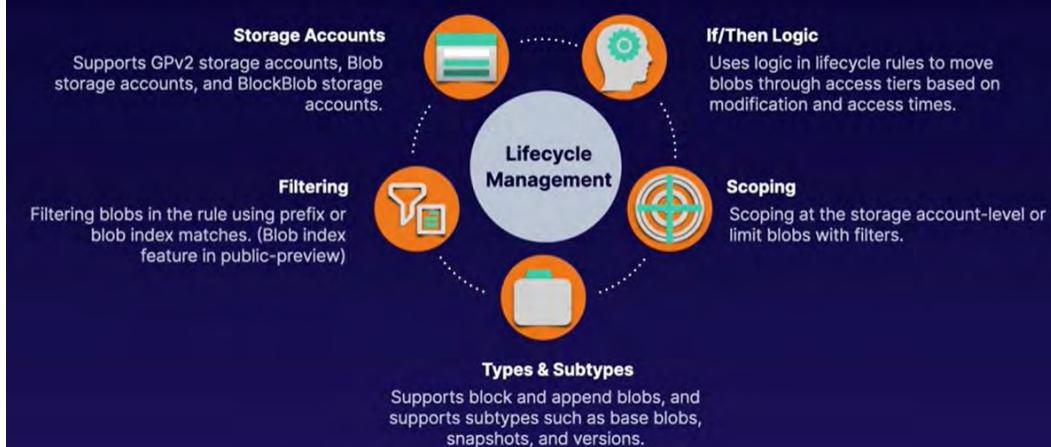


Pra ahorrar defines reglas, si el blob no ha sido accesado en días lo puedes mover a cool y de cool a archive y de archive se puede eliminar dependiendo de las reglas que definas.

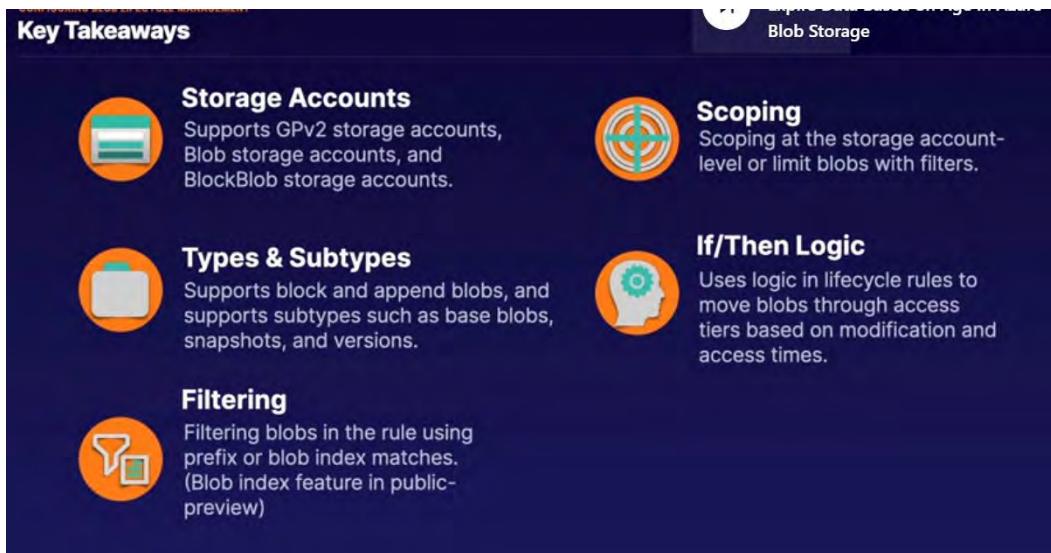
Access tracking es cuando regresas de cool a hot un blob.(Solo esta en algunas regiones)

Features of Lifecycle Management

A CLOUD GURU



Solo block blobs y append blobs son soportados por este feature(page blobs no)



- **If:** The If clause sets the evaluation clause for the policy rule. When the **If clause evaluates to true**, the **Then clause is executed**. Use the If clause to set the time period to apply to the blob data. The lifecycle management feature checks if the data is accessed or modified according to the specified time.
 - **More than (days ago):** The number of days to use in the evaluation condition.
- **Then:** The **Then clause sets the action clause for the policy rule**. When the If clause evaluates to true, the Then clause is executed. Use the Then clause to set the transition action for the blob data. The lifecycle management feature transitions the data based on the setting.
 - **Move to cool storage:** The blob data is transitioned to Cool tier storage.
 - **Move to archive storage:** The blob data is transitioned to Archive tier storage.
 - **Delete the blob:** The blob data is deleted.

Configuring Azure Files

Azure Files

Azure Files is a sub-service/sub-resource of Azure Storage (storage accounts).

Azure Files is a managed file share service.

Features:

- SMB connectivity
- Supports Windows, Linux, and macOS
- Extended by Azure File Sync



File Service

Azure Files service is a sub-service of Azure Storage storage accounts.



File Share

The file structure we are connecting to locally.

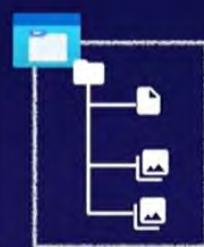
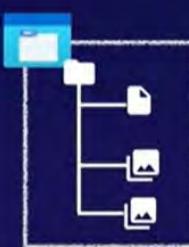


Files and Folders

The files and folders that exist in the file share.



Storage Account



File Share 1

File Share 2

Podemos tener múltiples file share en nuestra nube dentro de nuestra storage account

Para internal connectivity tenemos REST, SMB 2.1 Y SMB 3.0. Para la external connectivity igual pero no tenemos la 2.1 por que no esta encriptada la conexión

Connectivity Options**Internal Connectivity**

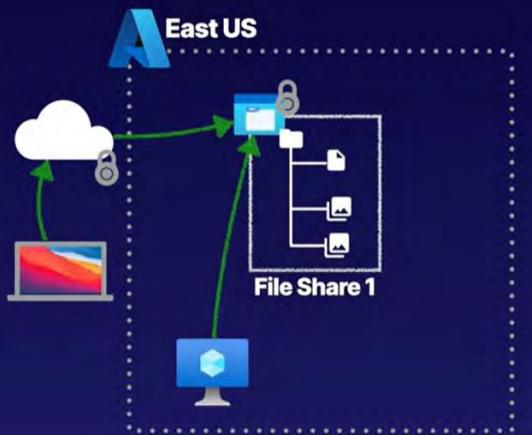
REST, SMB 2.1, and SMB 3.0

External Connectivity

REST and SMB 3.0

Security

Data encrypted at rest by default and in transit over HTTPS

**1****Managed File Share**

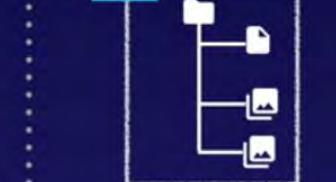
Utilizes storage account redundancy and security

2**Operating Systems**

Windows, Linux, and macOS support

3**File Share Quota**

5TB default size

Storage Account**File Share****Podemos tener hasta 100 TB de file shared**

Azure Files

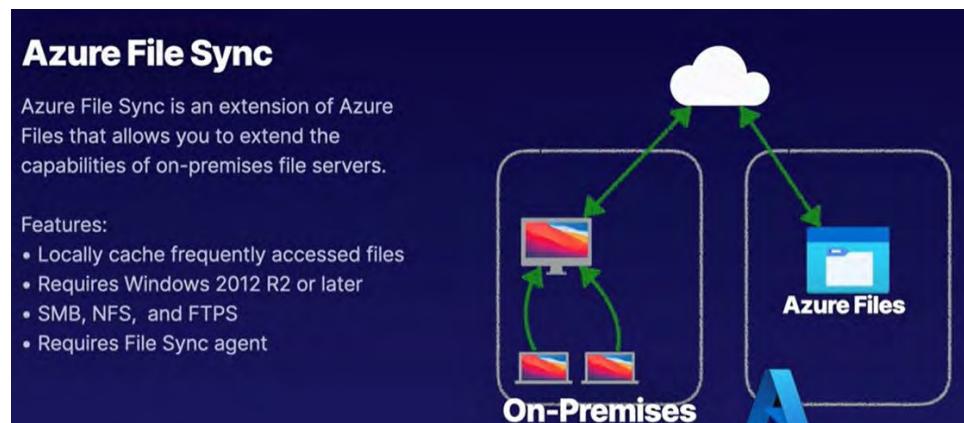
Azure Files enables you to set up highly available network file shares. Shares can be accessed by using the Server Message Block (SMB) protocol and the Network File System (NFS) protocol. Multiple virtual machines can share the same files with both read and write access. You can also read the files by using the REST interface or the storage client libraries.

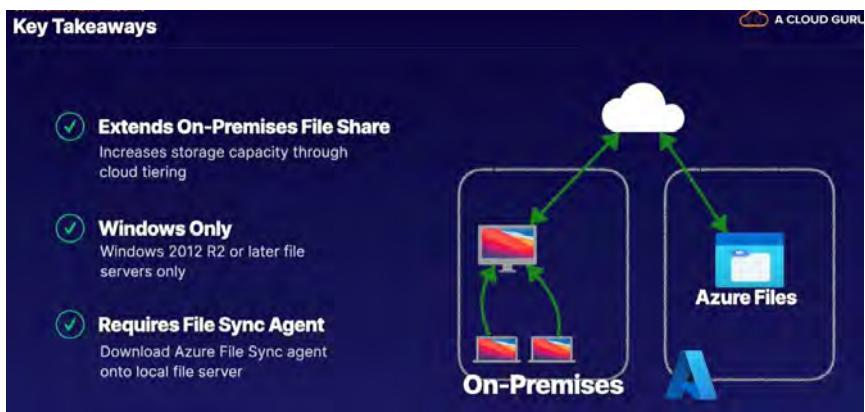
File shares can be used for many common scenarios:

- Many on-premises applications use file shares. This feature makes it easier to migrate those applications that share data to Azure. If you mount the file share to the same drive letter that the on-premises application uses, the part of your application that accesses the file share should work with minimal, if any, changes.
- Configuration files can be stored on a file share and accessed from multiple virtual machines. Tools and utilities used by multiple developers in a group can be stored on a file share, ensuring that everybody can find them, and that they use the same version.
- Diagnostic logs, metrics, and crash dumps are just three examples of data that can be written to a file share and processed or analyzed later.

The storage account credentials are used to provide authentication for access to the file share. All users who have the share mounted should have full read/write access to the share.

Configuring Azure File sync





Things to consider when using Azure Files

There are many common scenarios for using Azure Files storage. As you review the following suggestions, think about how Azure Files storage can provide solutions for your organization.

- Consider replacement and supplement options. Replace or supplement traditional on-premises file servers or NAS devices by using Azure Files.
- Consider global access. Directly access Azure Files shares by using most operating systems, such as Windows, macOS, and Linux from anywhere in the world.
- Consider lift and shift support. Lift and shift applications to the cloud with Azure Files for apps that expect a file share to store file application or user data.
- Consider the Azure File Sync agent. Replicate Azure Files shares to Windows Servers by using the Azure File Sync agent. You can replicate on-premises or in the cloud for performance and distributed caching of the data where it's being used. We'll take a closer look at the agent in a later unit.
- Consider shared applications. Store shared application settings in Azure Files, such as configuration files.
- Consider diagnostic data. Use Azure Files to store diagnostic data such as logs, metrics, and crash dumps in a shared location.
- Consider tools and utilities. Azure Files is a good option for storing tools and utilities that are needed for developing or administering Azure Virtual Machines or cloud services.

Azure Files (file shares)	Azure Blob Storage (blobs)	Azure Disks (page blobs)
Azure Files provides the SMB and NFS protocols, client libraries, and a REST interface that allows access from anywhere to stored files.	Azure Blob Storage provides client libraries and a REST interface that allows unstructured data to be stored and accessed at a massive scale in block blobs.	Azure Disks is similar to Azure Blob Storage. Azure Disks provides a REST interface to store and access index-based or structured data in page blobs.
- Files in an Azure Files share are true directory objects. - Data in Azure Files is accessed through file shares across multiple virtual machines.	- Blobs in Azure Blob Storage are a flat namespace. - Blob data in Azure Blob Storage is accessed through a container.	- Page blobs in Azure Disks are stored as 512-byte pages. - Page blob data is exclusive to a single virtual machine.
Azure Files is ideal to lift and shift an application to the cloud that already uses the native file system APIs. Share data between the app and other applications running in Azure. Azure Files is a good option when you want to store development and debugging tools that need to be accessed from many virtual machines.	Azure Blob Storage is ideal for applications that need to support streaming and random-access scenarios. Azure Blob Storage is a good option when you want to be able to access application data from anywhere.	Azure Disks solutions are ideal when your applications run frequent random read/write operations. Azure Disks is a good option when you want to store relational data for operating system and data disks in Azure Virtual Machines and databases.

Things to consider when using Azure Files shares

There are two important settings for Azure Files that you need to be aware of when creating and configuring file shares.

- Open port 445. Azure Files uses the SMB protocol. SMB communicates over TCP port 445. Be sure port 445 is open. Also, make sure your firewall isn't blocking TCP port 445 from the client machine.
- Enable secure transfer. The secure transfer required setting enhances the security of your storage account by limiting requests to your storage account from secure connections only. Consider the scenario where you use REST APIs to access your storage account. If you attempt to connect, and secure transfer required is enabled, you must connect by using HTTPS. If you try to connect to your account by using HTTP, and secure transfer required is enabled, the connection is rejected.

Mount Azure Files share on Linux

You can also connect Azure Files shares with Linux machines. From your virtual machine page, select Connect. Azure Files shares can be mounted in Linux distributions by using the CIFS kernel client. File mounting can be done on-demand with the mount command or on-boot (persistent) by creating an entry in /etc/fstab.

The screenshot shows a configuration interface for mounting an Azure Files share on a Linux machine. At the top, there are tabs for Windows, Linux (which is selected), and macOS. Below the tabs, a 'Mount point' input field contains the value 'testr'. A note below the input field says, 'To connect to this file share from a Linux computer, run this command:'. A 'Show Script' button is present. A detailed note below states: 'In order to mount an Azure file share outside of the Azure region it is hosted in, such as on-premises or in a different Azure region, the OS must support the encryption functionality of SMB 3.0.' At the bottom, a link 'Learn more about Azure File Storage with Linux' is visible.

Things to know about file share snapshots

Let's review some characteristics of file share snapshots.

- The Azure Files share snapshot capability is provided at the file share level.
- Share snapshots are incremental in nature. Only data changed since the most recent share snapshot is saved.
- Incremental snapshots minimize the time required to create share snapshots and saves on storage costs.
- Even though share snapshots are saved incrementally, you only need to retain the most recent share snapshot to restore the share.
- You can retrieve a share snapshot for an individual file. This level of support helps with restoring individual files rather than having to restore to the entire file share.
- If you want to delete a share that has share snapshots, you must first delete all its snapshots.

Implement Azure File Sync

✓ 100 XP

3 minutes

Azure File Sync enables you to cache several Azure Files shares on an on-premises Windows Server or cloud virtual machine. You can use Azure File Sync to centralize your organization's file shares in Azure Files, while keeping the flexibility, performance, and compatibility of an on-premises file server.



Things to know about Azure File Sync

Let's take a look at the characteristics of Azure File Sync.

- Azure File Sync transforms Windows Server into a quick cache of your Azure Files shares.
- You can use any protocol that's available on Windows Server to access your data locally with Azure File Sync, including SMB, NFS, and FTPS.
- Azure File Sync supports as many caches as you need around the world.

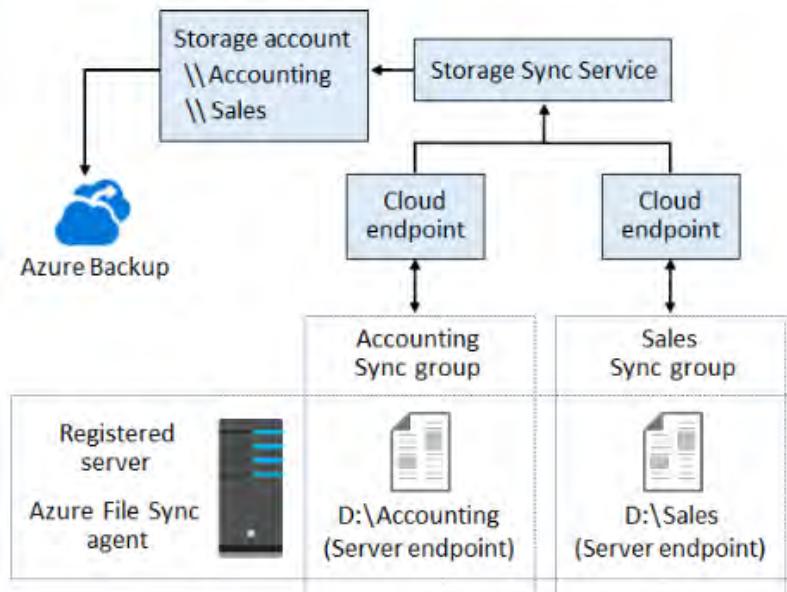
Identify Azure File Sync components

✓ 100 XP

3 minutes

Azure File Sync is composed of four main components that work together to provide caching for Azure Files shares on an on-premises Windows Server or cloud virtual machine.

The following illustration shows how the components of Azure File Sync provide a cache for a storage account that has Accounting and Sales data stored in Azure Files shares.



Deploy Azure File Sync

✓ 100 XP

2 minutes

Before you can start synchronizing files with Azure File Sync, there are several high-level steps that need to be completed.

- ① Deploy Storage Sync Service
- ② Prepare Windows Server(s)
- ③ Install Azure File Sync agent
- ④ Register Windows Server(s)

Choose the best response for each of the questions below. Then select **Check your answers**.

1. Which of the following statements correctly describes cloud tiering?

- Cloud tiering prioritizes the sync order of file shares.
- Cloud tiering sets the frequency at which the sync job runs.
X Incorrect. Cloud tiering doesn't set the job frequency.
- Cloud tiering archives infrequently accessed files to free up space on the local file share.
✓ Correct. Cloud tiering allows frequently accessed files to be cached on the local server.
Infrequently accessed files are tiered or archived to the Azure Files share according to the policy created.

2. What's the best way to sync files stored on the manufacturing warehouse machines with the cloud?

- Create an Azure Files share and directly mount shares on the machines in the warehouse.
- Use a machine in the warehouse to host a file share, install Azure File Sync, and share a drive with the rest of the warehouse.
✓ Correct. This answer is the best option. The low bandwidth means Azure File Sync can handle the updating and syncing of files efficiently over the low-bandwidth network.
- Install Azure File Sync on every machine in the warehouse and also in the main office.

3. How is the Azure File Sync agent installed and used?

- The Azure File Sync agent is installed on a server to enable Azure File Sync replication between the local file share and an Azure Files share.
✓ Correct. The Azure File Sync agent is a downloadable package that enables a Windows Server file share to be synced with an Azure Files share.
- The Azure File Sync agent is installed on a server to set NTFS permissions on files and folders.
- The Azure File Sync agent is installed on an Azure Files share to control on-premises file and folder replication traffic.

1. Suppose you have two video files stored as blobs. One of the videos is business-critical and requires a replication policy that creates multiple copies across geographically diverse datacenters. The other video is non-critical, and a local replication policy is sufficient. Which of the following options would satisfy both data diversity and cost sensitivity consideration.

- Create a single storage account that makes use of Local-redundant storage (LRS) and host both videos from here.
- Create a single storage account that makes use of Geo-redundant storage (GRS) and host both videos from here.

Create two storage accounts. The first account makes use of Geo-redundant storage (GRS) and hosts the business-critical video content. The second account makes use of Local-redundant storage (LRS) and hosts the non-critical video content.

- In general, increased diversity means an increased number of storage accounts. A storage account by itself has no financial cost. However, the settings you choose for the account do influence the cost of services in the account. Use multiple storage accounts to reduce costs.

2. The name of a storage account must be:

- Unique within the containing resource group.
- Unique within your Azure subscription.
- Globally unique.

- The storage account name is used as part of the URI for API access, so it must be globally unique.

3. In a typical project, when would you create your storage account(s)?

- At the beginning, during project setup.
 - Storage accounts are stable for the lifetime of a project. It's common to create them at the start of a project.
- After deployment, when the project is running.
- At the end, during resource cleanup.

What is Azure Queue Storage?

Article • 11/21/2022 • 11 contributors

 Feedback

In this article

[Queue Storage concepts](#)

[Next steps](#)

Azure Queue Storage is a service for storing large numbers of messages. You access messages from anywhere in the world via authenticated calls using HTTP or HTTPS. A queue message can be up to 64 KB in size. A queue may contain millions of messages, up to the total capacity limit of a storage account. Queues are commonly used to create a backlog of work to process asynchronously.

- Message: A message, in any format, of up to 64 KB. Before version 2017-07-29, the maximum time-to-live allowed is seven days. For version 2017-07-29 or later, the maximum time-to-live can be any positive number, or -1 indicating that the message doesn't expire. If this parameter is omitted, the default time-to-live is seven days.

Queue

- Container for messages
- **Up to 500 TiB** of data
- **Max 2,000** (1KiB) messages/s

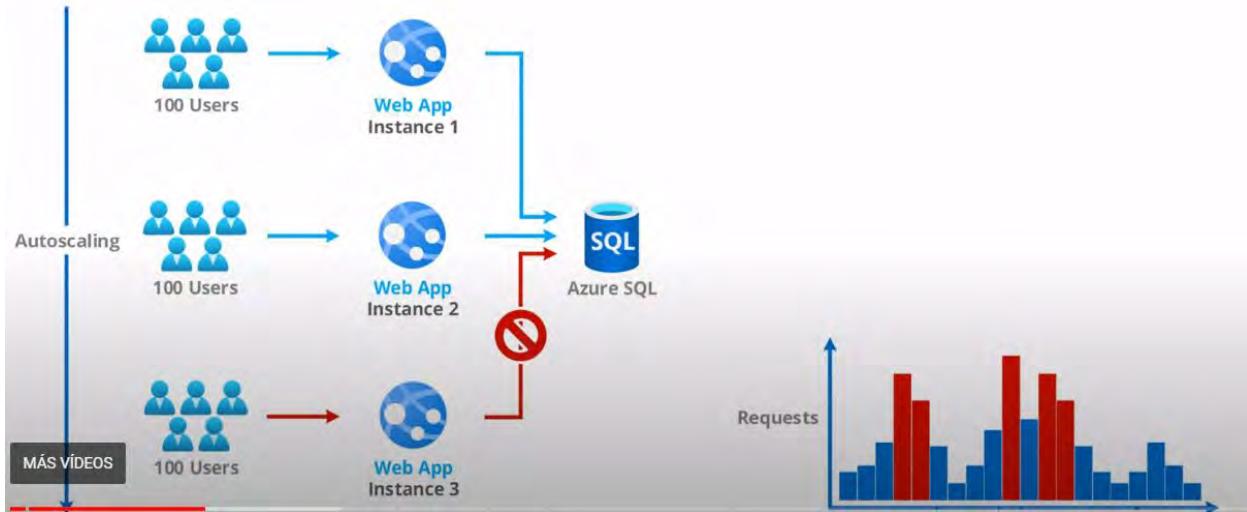
Message

- A data in **any format**
- **Up to 64 KB**
- **Default time-to-live (TTL) is 7 days**
- Non-expiring messages (TTL of -1)



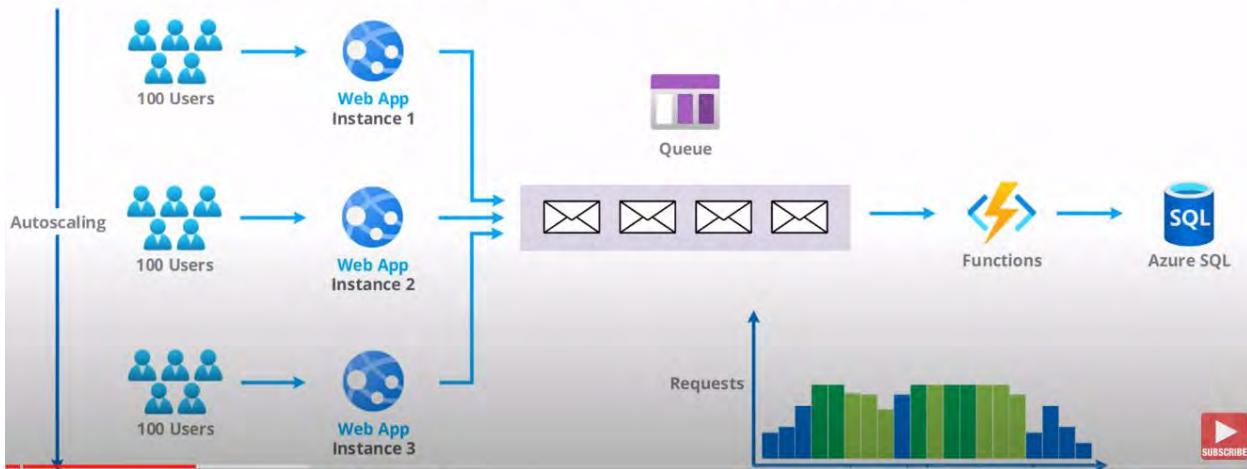
Why Queues?

Ver más ta...

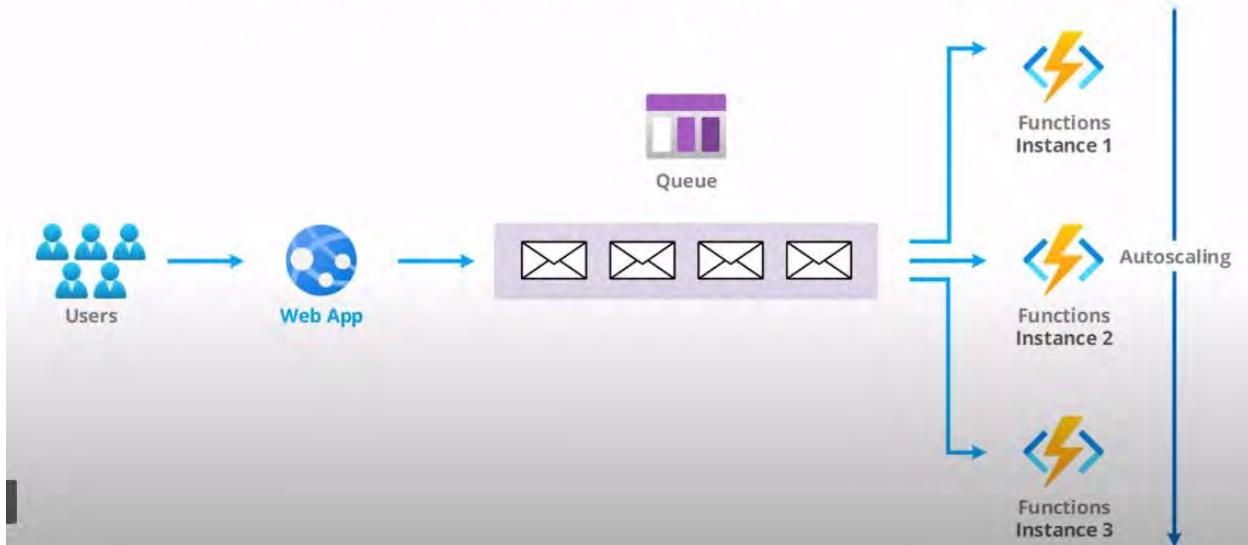


Why Queues?

Queue-Based Load Leveling pattern



Competing Consumers pattern (fan-out)



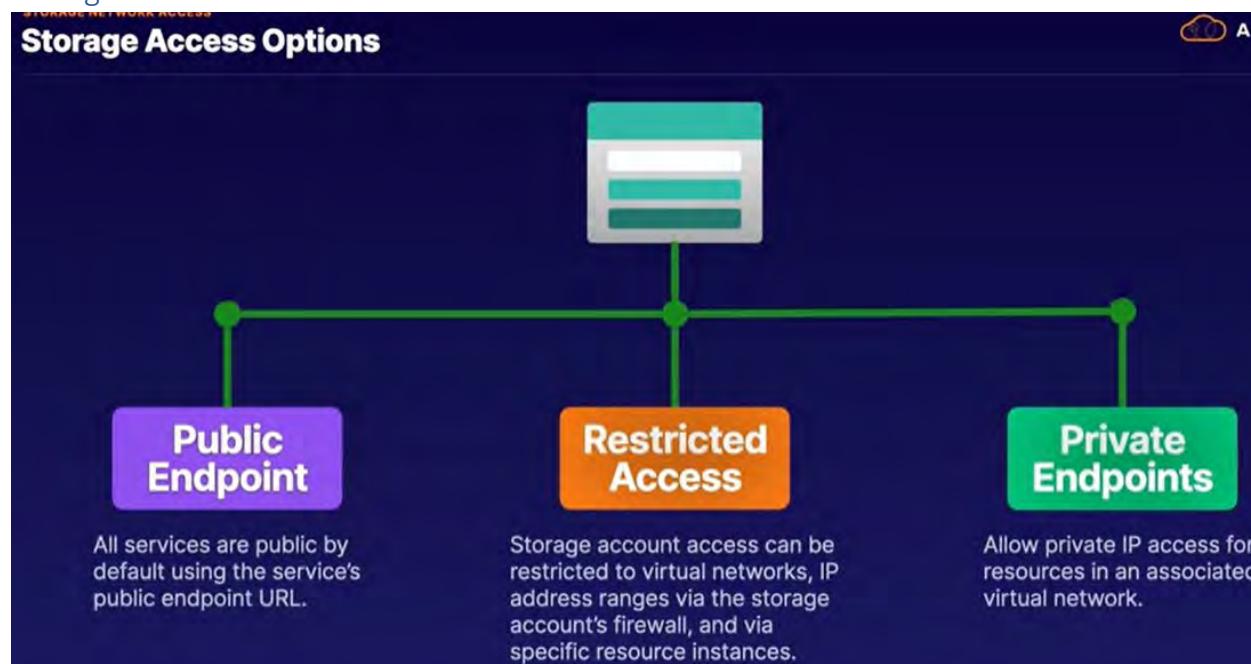
Azure Table Storage

Azure Table Storage (Azure Cosmos DB)

Azure Table Storage is a fully managed NoSQL database service for modern app development. As a fully managed service, Azure Cosmos DB takes database administration off your hands with automatic management, updates, and patching. It also handles capacity management with cost-effective serverless and automatic scaling options that respond to application needs to match capacity with demand.

In addition to the existing Azure Table Storage service, there's a new Azure Cosmos DB Table API offering that provides throughput-optimized tables, global distribution, and automatic secondary indexes.

Storage Network Access



El que esta por default es el public endpoint

En networking podemos definir el acceso a los containers y blobs:

Screenshot of the Azure Storage account Networking settings page for 'clouddemochaseshell'.

Firewalls and virtual networks tab is selected.

Allow access from:
 All networks Selected networks
All networks, including the internet, can access this storage account.

Network Routing
Determine how you would like to route your traffic as it travels from its source to an Azure endpoint.

Routing preference: Microsoft network routing Internet routing

Publish route-specific endpoints:
 Microsoft network routing
 Internet routing

Networking is selected in the left sidebar under Security + networking.

Securing Storage accounts

Azure Storage Encryption

Secure Storage

By default, all data stored (data at rest) in any Azure Storage service is secured using Storage Service Encryption (SSE).

All data in transit can be secured using transport-level security (HTTPS).

Azure Storage Authentication

The diagram illustrates the Azure Storage Architecture. It features two main layers: the **Management Layer** (orange box) and the **Data Layer** (blue box). The Management Layer contains a central teal hexagon icon and a green server icon. The Data Layer contains four blue square icons representing different storage services. A green arrow points from the Management Layer to the Data Layer, indicating the flow of management control.

- Access Keys**
Azure-generated keys that provide unlimited access to both the management and data layer of an Azure Storage solution.
- Shared Access Signature (SAS)**
An access signature, generated from access keys, that provides limited access at either the account level or the service level.
- Azure AD Authentication**
Uses Azure role-based access control (RBAC) and Azure Active Directory (AD) identities to provide authentication (instead of access keys).

Storage account

Search (Cmd +/)

Successfully regenerated access key 'key1' for storage account 'clouddemochaseshell'.

Networking

Azure CDN

Access keys

Shared access signature

Encryption

Security

management

Geo-replication

Data protection

Object replication

Blob inventory (preview)

Static website

Lifecycle management

Azure search

Storage account name: clouddemochaseshell

key1

Key: 4IJ8IL+7vCcZOf73p2ZVZ/Rml/MF+OZnTN8phdt+OsEHENCsWToWAjL8C3OhZQ427VKOjaffbeeY6JS8X8cKQ==

Connection string: DefaultEndpointsProtocol=https;AccountName=clouddemochaseshell;AccountKey=4IJ8IL+7vCcZOf73p2ZVZ/Rml/MF+OZnTN8phdt+OsEHENCsWToWAjL8C3...

key2

Key: TsDqW61L6s1hKa+zon45Slj7AcGW1C1f6Y6yxW7F21vqeEQo3LXjEha2j3Fk47lWEr41TNZ8mn8UTih3w/Q==

Connection string: DefaultEndpointsProtocol=https;AccountName=clouddemochaseshell;AccountKey=TsDqW61L6s1hKa+zon45Slj7AcGW1C1f6Y6yxW7F21vqeEQo3LXjEha2j3Fk...

El sas token se puede generar a nivel de servicio, blob o de storage account

Azure defender for storage nos dara recomendaciones para vulnerabilidades

Storage account

Search (Cmd +/)

Azure Defender for Storage

Azure Defender for Storage detects potentially harmful attempts to access or exploit Blob containers and File shares in your storage accounts.

Enjoy a 30-day free trial. When the trial ends, you'll be charged \$0.02 per 10,000 transactions in Blob containers and File shares.

Your account currently processes approximately 11 transactions per second.

Enable Azure Defender for Storage

Recommendations

Security Center continuously monitors the configuration of your storage accounts to identify potential security vulnerabilities and recommends actions to mitigate them.

No recommendations to display

and recommend the actions we can take to mitigate those.

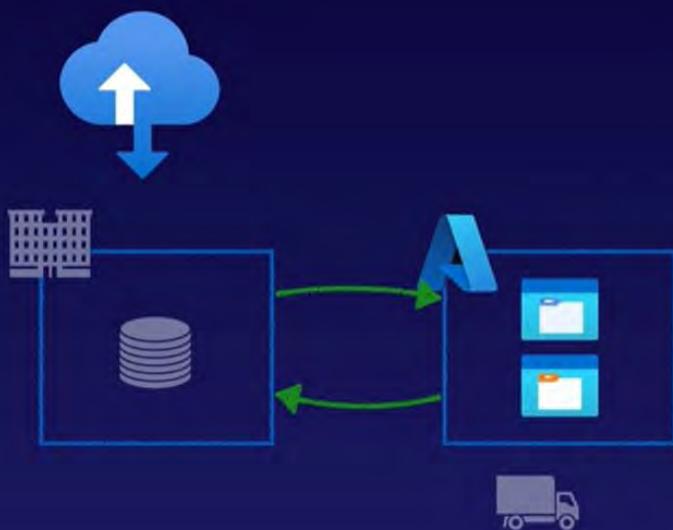
Desde azure storage explorer puedes acceder a blobs con un sas token

Using Azure Jobs

Basicamente es mover discos físicos de data de on premise a la nube o viceversa y como tal los empaquetas y los envias. File Service solo es de on premise a la nube

Describing Azure Jobs

A CLOUD



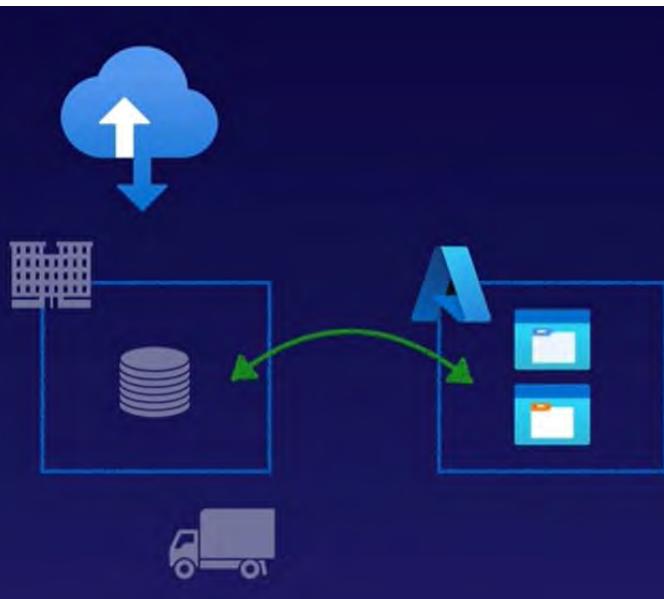
Azure Jobs

Move large amounts of data between on-premises and Azure Storage.

- Move to/from Blob service
- Move to Files service
- Transport self-supplied drive

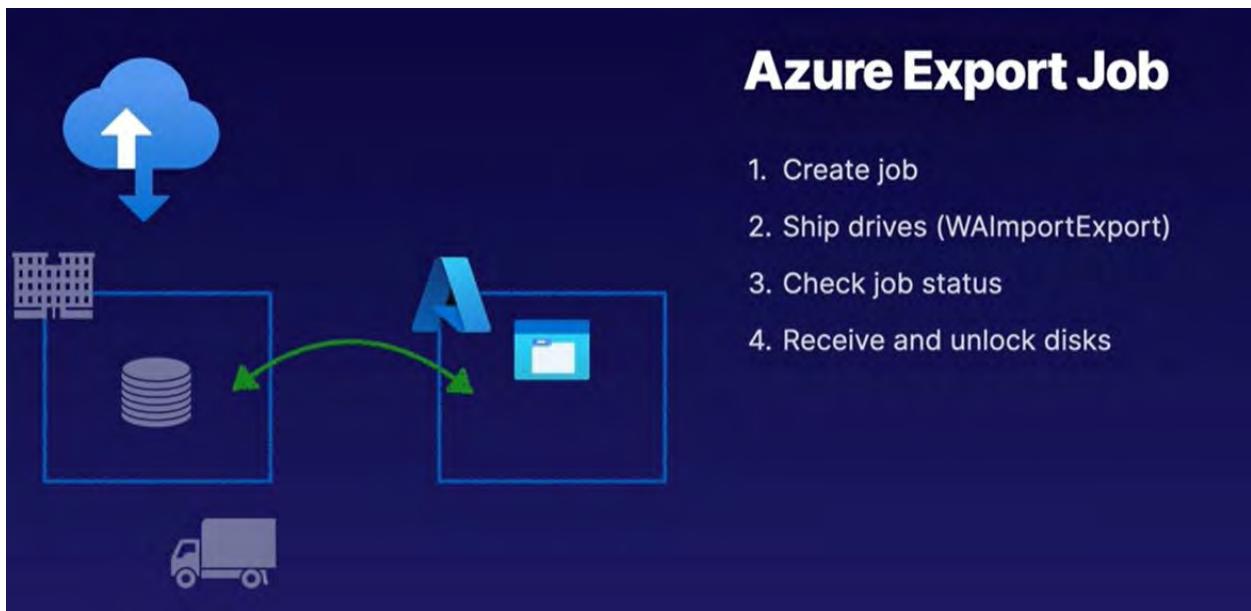
Supported drive types:

- SATA
- HDD
- SSD



Azure Import Job

1. Prepare disks (WAIimportExport)
2. Create job
3. Ship drives
4. Check job status
5. Receive disks
6. Check data in Azure Storage



Para crear uno nos vamos a import/export Jobs en la barra de búsquedas

 Import Jobs Send large amounts of data to the Azure cloud when network bandwidth won't support data migration.	 WAImportExport CLI Tool Use to prepare disks for data and to estimate number of disks needed.
 Export Jobs Receive large amounts of data on-premises from the Azure cloud when network bandwidth won't support data migration.	 Windows Support Only
	 Azure Blob and Files

Things to know about the WAImportExport tool

You can use the WAImportExport tool with the Azure Import/Export service to complete the following tasks:

- Before you create an Azure Import job, use the WAImportExport tool to copy data to the hard disk drives you intend to ship to Microsoft.
- After your Azure Import job completes, use the WAImportExport tool to repair any blobs that were corrupted, missing, or that have conflicts with other blobs in your Azure Storage.
- After you receive your disk drives from a completed Azure Export job, use the WAImportExport tool to repair any corrupted or missing files on the drives.
- The WAImportExport tool handles data copy, volume encryption, and creation of journal files. Journal files are necessary to create an Azure Import/Export job and help ensure the integrity of the data transfer.

Things to consider when using the WAImportExport tool

There are several points to consider as you plan for using the WAImportExport tool with the Azure Import/Export service.

- Consider supported disk drives. For hard disk drives, the Azure Import/Export service requires internal SATA II/III HDDs or SSDs. Keep this requirement in mind when selecting your hard disk drives.
- Consider BitLocker encryption. When you prepare a disk for an Azure Import job, you must encrypt the NTFS volume of each disk drive with BitLocker.
- Consider OS version. To prepare a disk drive, you must connect the drive to a computer that's running a 64-bit version of the Windows client or server operating system. You run the WAImportExport tool from that computer.

Storage Utilities

STORAGE UTILITIES

Describing Utilities



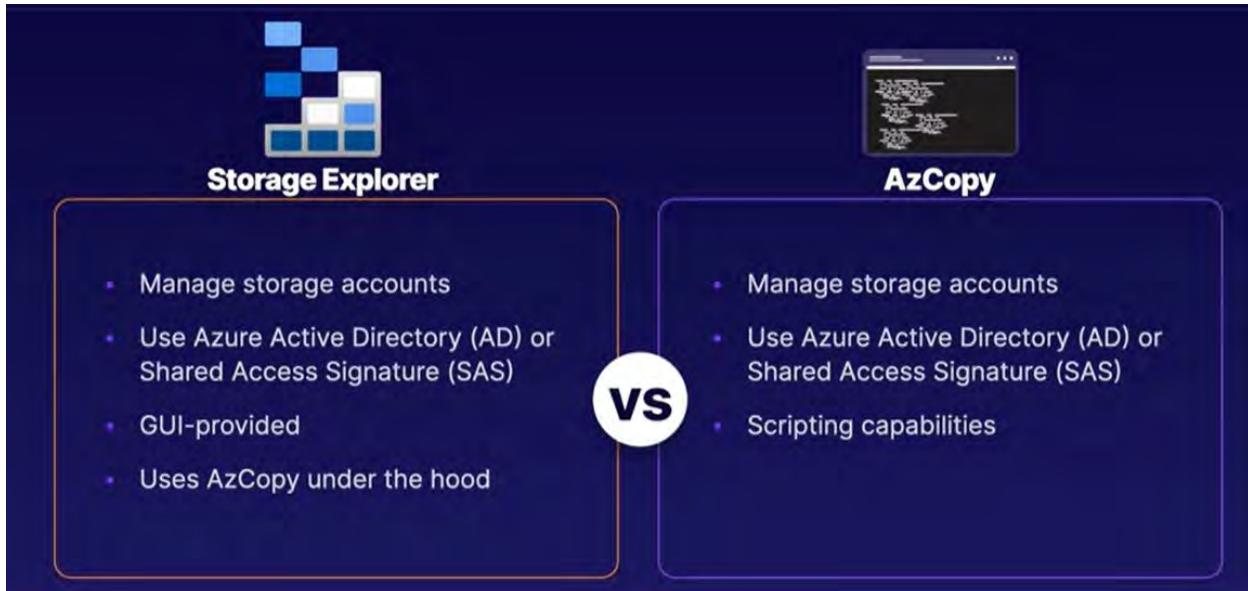
Storage Explorer
A Graphical User Interface (GUI) tool for working with storage accounts. Supported for Windows, Linux, and MacOS.



AzCopy
A command-line utility for working with storage accounts. Supported for Windows, Linux, and MacOS.

Storage explorer se descarga y desde ahí puedes manejar las storage accounts sin entrar al portal de azure

AzCopy se descarga y hay que autorizarlo usando credenciales de AD o usando un SAS. Básicamente manejas los blobs y storage accounts desde líneas de comandos



Things to know about AzCopy

Let's look at some of the characteristics of the AzCopy tool.

- Every AzCopy instance creates a job order and a related log file. You can view and restart previous jobs, and resume failed jobs.
- You can use AzCopy to list or remove files or blobs in a given path. AzCopy supports wildcard patterns in a path, `--include` flags, and `--exclude` flags.
- AzCopy automatically retries a transfer when a failure occurs.
- When you use Azure Blob Storage, AzCopy lets you copy an entire account to another account. No data transfer to the client is needed.
- AzCopy supports Azure Data Lake Storage Gen2 APIs.
- AzCopy is built into Azure Storage Explorer.
- AzCopy is available on Windows, Linux, and macOS.

Knowledge check

✓ 200 XP

3 minutes

Your company maintains several types of Azure Storage in the various departments. You're tasked with designing a solution to maintain the storage by using different Azure Storage tools to support specific scenarios.

- The finance team needs to transfer a series of large files to Azure Blob Storage. The operation might take several hours to upload each file. The team is concerned about what happens if the transfer fails and the process has to be restarted.
- The manufacturing department wants to control how data is transferred to Azure Files. They want a graphical tool to manage the process, but they don't want to use the Azure portal.
- Your administrators maintain an existing storage account in Azure for unstructured data. For billing purposes, management has requested a new storage account for the data. The admins need to be sure no data is lost when moving to the new storage account.

Answer the following questions

Choose the best response for each of the questions below. Then select Check your answers.

1. Which storage approach can help resolve the concerns of the finance team?

The Azure CLI

AzCopy

✓ Correct. AzCopy is ideal for transferring large files because the tool can run in the background.

Azure Storage Explorer

2. What storage tool satisfies the request of the manufacturing department?

Azure Data Box

Robocopy

Azure Storage Explorer

✓ Correct. Azure Storage Explorer is the best choice for the manufacturing department because they don't want to access the files through the Azure portal.

3. How can admins move the data in the existing storage account to the new storage account?

Use the AzCopy command-line tool

✓ Correct. The key task for the admins is to move data between storage accounts. The AzCopy tool can work with two different storage accounts. The other tools don't copy data between storage accounts. Azure Storage Explorer is another tool that can be used to copy data between storage accounts.

Use the Azure portal

Use the Robocopy command-line tool

Things to know about Azure Storage security strategies

Let's look at some characteristics of Azure Storage security.

- **Encryption.** All data written to Azure Storage is automatically encrypted by using Azure Storage encryption.
- **Authentication.** Azure Active Directory (Azure AD) and role-based access control (RBAC) are supported for Azure Storage for both resource management operations and data operations.
 - Assign RBAC roles scoped to an Azure storage account to security principals, and use Azure AD to authorize resource management operations like key management.
 - Azure AD integration is supported for data operations on Azure Blob Storage and Azure Queue Storage.
- **Data in transit.** Data can be secured in transit between an application and Azure by using Client-Side Encryption, HTTPS, or SMB 3.0.
- **Disk encryption.** Operating system disks and data disks used by Azure Virtual Machines can be encrypted by using Azure Disk Encryption.
- **Shared access signatures.** Delegated access to the data objects in Azure Storage can be granted by using a shared access signature (SAS).
- **Authorization.** Every request made against a secured resource in Blob Storage, Azure Files, Queue Storage, or Azure Cosmos DB (Azure Table Storage) must be authorized. Authorization ensures that resources in your storage account are accessible only when you want them to be, and to only those users or applications whom you grant access.

Authorization strategy	Description
Azure Active Directory	Azure AD is Microsoft's cloud-based identity and access management service. With Azure AD, you can assign fine-grained access to users, groups, or applications by using role-based access control.
Shared Key	Shared Key authorization relies on your Azure storage account access keys and other parameters to produce an encrypted signature string. The string is passed on the request in the Authorization header.
Shared access signatures	A SAS delegates access to a particular resource in your Azure storage account with specified permissions and for a specified time interval.
Anonymous access to containers and blobs	You can optionally make blob resources public at the container or blob level. A public container or blob is accessible to any user for anonymous read access. Read requests to public containers and blobs don't require authorization.

Things to know about shared access signatures

Let's review some characteristics of a SAS.

- A SAS gives you granular control over the type of access you grant to clients who have the SAS.
- An account-level SAS can delegate access to multiple Azure Storage services, such as blobs, files, queues, and tables.
- You can specify the time interval for which a SAS is valid, including the start time and the expiration time.
- You specify the permissions granted by the SAS. A SAS for a blob might grant read and write permissions to that blob, but not delete permissions.
- SAS provides account-level and service-level control.
 - Account-level SAS delegates access to resources in one or more Azure Storage services.
 - Service-level SAS delegates access to a resource in only one Azure Storage service.

① Note

A stored access policy can provide another level of control when you use a service-level SAS on the server side.
You can group SASs and provide other restrictions by using a stored access policy.

- There are optional SAS configuration settings:
 - IP addresses. You can identify an IP address or range of IP addresses from which Azure Storage accepts the SAS. Configure this option to specify a range of IP addresses that belong to your organization.
 - Protocols. You can specify the protocol over which Azure Storage accepts the SAS. Configure this option to restrict access to clients by using HTTPS.

When you create your shared access signature (SAS), a uniform resource identifier (URI) is created by using parameters and tokens. The URI consists of your Azure Storage resource URI and the SAS token.



Parameter	Example	Description
Resource URI	<code>https://myaccount.blob.core.windows.net/?restype=service&comp=properties</code>	Defines the Azure Storage endpoint and other parameters. This example defines an endpoint for Blob Storage and indicates that the SAS applies to service-level operations. When the URI is used with <code>GET</code> , the Storage properties are retrieved. When the URI is used with <code>SET</code> , the Storage properties are configured.
Storage version	<code>sv=2015-04-05</code>	For Azure Storage version 2012-02-12 and later, this parameter indicates the version to use. This example indicates that version 2015-04-05 (April 5, 2015) should be used.
Storage service	<code>ss=bf</code>	Specifies the Azure Storage to which the SAS applies. This example indicates that the SAS applies to Blob Storage and Azure Files.
Start time	<code>st=2015-04-29T22%3A18%3A26Z</code>	(Optional) Specifies the start time for the SAS in UTC time. This example sets the start time as April 29, 2015 22:18:26 UTC. If you want the SAS to be valid immediately, omit the start time.
Expiry time	<code>se=2015-04-30T02%3A23%3A26Z</code>	Specifies the expiration time for the SAS in UTC time. This example sets the expiry time as April 30, 2015 02:23:26 UTC.
Resource	<code>sr=b</code>	Specifies which resources are accessible via the SAS. This example specifies that the accessible resource is in Blob Storage.
Permissions	<code>sp=rw</code>	Lists the permissions to grant. This example grants access to read and write operations.
IP range	<code>sip=168.1.5.60-168.1.5.70</code>	Specifies a range of IP addresses from which a request is accepted. This example defines the IP address range 168.1.5.60 through 168.1.5.70.
Protocol	<code>spr=https</code>	Specifies the protocols from which Azure Storage accepts the SAS. This example indicates that only requests by using HTTPS are accepted.
Signature	<code>sig=f%6GRVAZ5Cdj2Pw4tgU7I1STkWgn7bUkkAg8P6HESXwmf%4B</code>	Specifies that access to the resource is authenticated by using an HMAC signature. The signature is computed over a string-to-sign with a key by using the SHA256

Things to know about Azure Storage encryption

Examine the following characteristics of Azure Storage encryption.

- Data is encrypted automatically before it's persisted to Azure Managed Disks, Azure Blob Storage, Azure Queue Storage, Azure Cosmos DB, Azure Table Storage, or Azure Files.
- Data is automatically decrypted before it's retrieved.
- Azure Storage encryption, encryption at rest, decryption, and key management are transparent to users.
- All data written to Azure Storage is encrypted through 256-bit advanced encryption standard (AES) encryption. AES is one of the strongest block ciphers available.
- Azure Storage encryption is enabled for all new and existing storage accounts and can't be disabled.

100 XP

Create customer-managed keys

2 minutes

For your Azure Storage security solution, you can use Azure Key Vault to manage your encryption keys. The Azure Key Vault APIs can be used to generate encryption keys. You can also create your own encryption keys and store them in a key vault.

Things to know about customer-managed keys

Consider the following characteristics of customer-managed keys.

- By creating your own keys (referred to as *customer-managed keys*), you have more flexibility and greater control.
- You can create, disable, audit, rotate, and define access controls for your encryption keys.
- Customer-managed keys can be used with Azure Storage encryption. You can use a new key or an existing key vault and key. The Azure storage account and the key vault must be in the same region, but they can be in different subscriptions.

It's important to understand that when you use a SAS in your application, there can be potential risks.

- If a SAS is compromised, it can be used by anyone who obtains it, including a malicious user.
- If a SAS provided to a client application expires and the application is unable to retrieve a new SAS from your service, the application functionality might be hindered.

1. Which solution is the easiest way to implement secure storage for the company's media files?

- Create a shared access signature (SAS) for each user and delete the SAS to prevent access.
- Create stored access policies for each container to enable revocation of access or change of duration.
 - ✓ Correct. The SAS changes access based on permissions or duration by replacing the stored access policy with a new one, or by deleting the stored access policy altogether to revoke access.
- Periodically regenerate the account key to control access to the files.

2. What's the default network rule when configuring network access to an Azure storage account?

- Allow all connections from all networks.
 - ✓ Correct. The default network rule is to allow all connections from all networks.
- Allow all connection from a private IP address range.
 - ✗ Incorrect. By default, the IP address isn't considered.
- Deny all connections from all networks.

3. What's the best way to implement secure access to Azure Storage for the company's users?

- Use shared access signatures for the production applications.
- Use access keys for the production applications.
 - ✓ Correct. Access keys provide unrestricted access to the storage resources, which is the requirement for production applications in this scenario.
- Use stored access policies for the production applications.

Check your knowledge

1. Your organization has an internal system to share patient appointment information and notes. You can secure a user's access based on their membership in an Azure Active Directory (Azure AD) group. Which kind of authorization supports this scenario best, and why?

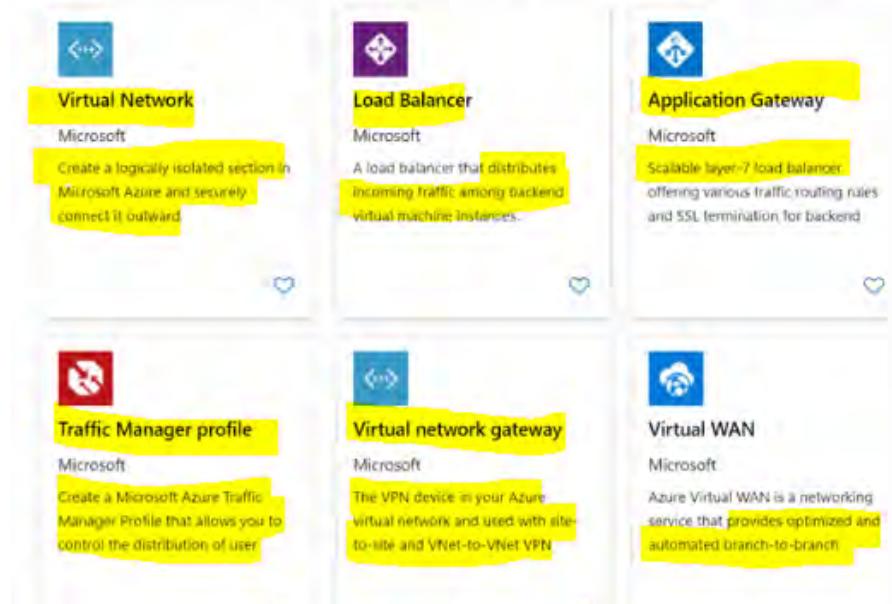
- Use a shared access signature (SAS) token. You use the Azure AD credentials and a user delegation SAS token.
- Use Azure Active Directory. By using Azure AD, you can create a service principal to authenticate the app.
 - ✓ This option is the best because no code or configuration files need to store credentials. Access is controlled with Azure AD and can be extended or revoked without requiring any code changes.
- Use a shared key. The Azure Storage account can create and revoke keys that will be used in your app.

2. Your public-facing static website stores **all** its public UI images in blob storage. The website needs to display the graphics without any kind of authorization. Which is the best option?

- Public access
 - ✓ This option requires the least effort to implement. There are no credentials that need to be stored or managed. For this website, it's the best option.
- Shared key
- Shared access signature

Conceptualizing Virtual Networking

After resources are moved to Azure, they require the same networking functionality as an on-premises deployment. In specific scenarios, the resources require some level of network isolation. Azure network services offer a range of components with functionalities and capabilities, as shown in the following image:

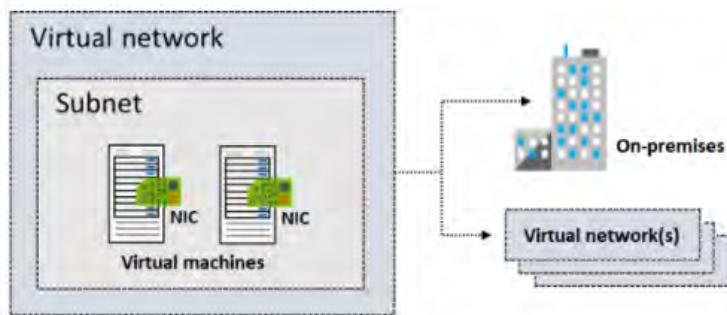


Things to know about Azure virtual networks

You can implement Azure Virtual Network to create a virtual representation of your network in the cloud. Let's examine some characteristics of virtual networks in Azure.

- An Azure virtual network is a logical isolation of the Azure cloud that's dedicated to your subscription.
- You can use virtual networks to provision and manage virtual private networks (VPNs) in Azure.
- Each virtual network has its own Classless Inter-Domain Routing (CIDR) block and can be linked to other virtual networks and on-premises networks.
- You can link virtual networks with an on-premises IT infrastructure to create hybrid or cross-premises solutions, when the CIDR blocks of the connecting networks don't overlap.
- You control the DNS server settings for virtual networks, and segmentation of the virtual network into subnets.

The following illustration depicts a virtual network that has a subnet containing two virtual machines. The virtual network has connections to an on-premises infrastructure and a separate virtual network.



Things to consider when using virtual networks

Virtual networks can be used in many ways. As you think about the configuration plan for your virtual networks and subnets, consider the following scenarios.

Scenario	Description
Create a dedicated private cloud-only virtual network	Sometimes you don't require a cross-premises configuration for your solution. When you create a virtual network, your services and virtual machines within your virtual network can communicate directly and securely with each other in the cloud. You can still configure endpoint connections for the virtual machines and services that require internet communication, as part of your solution.
Securely extend your data center with virtual networks	You can build traditional site-to-site VPNs to securely scale your datacenter capacity. Site-to-site VPNs use IPSEC to provide a secure connection between your corporate VPN gateway and Azure.
Enable hybrid cloud scenarios	Virtual networks give you the flexibility to support a range of hybrid cloud scenarios. You can securely connect cloud-based applications to any type of on-premises system, such as mainframes and Unix systems.

Describing Networks



Traditional On-Premises Network



Purpose of a Network

A network allows you to have an isolated network where resources can communicate with one another and with outside networks.

- Users accessing file servers
- Printer sharing
- Web servers
- App server accessing database servers and internet

Network security group puede controlar private and public networking. Se ponen a nivel subnet.

Describing Virtual Networks (VNets)



1

Isolated Network

VNets are isolated networks on the Azure cloud

2

Private Network Access

Provides private connectivity between resources like VMs or App Service

3

Network Integration

Allows connectivity between VNets, on-prem networks, and remote user devices

Componentes de una vnet:

Components of Virtual Networks



Address Space

The private address space for the isolated network. Required to provide resources with private IPs.



VNet

The isolated network on Azure cloud where Azure resources like VMs are deployed.



Subnet

The segmentation of the isolated network into smaller sub-networks where resources will exist.

Creating Virtual networks

Designing a Network



Determine IP CIDR

Select a Classless Inter-Domain Routing (CIDR) notation that allows for growth and integration.



Subnetting Requirements

Determine how to segment the solution to meet your needs, such as segmenting for n-tiers.



Connectivity Needs

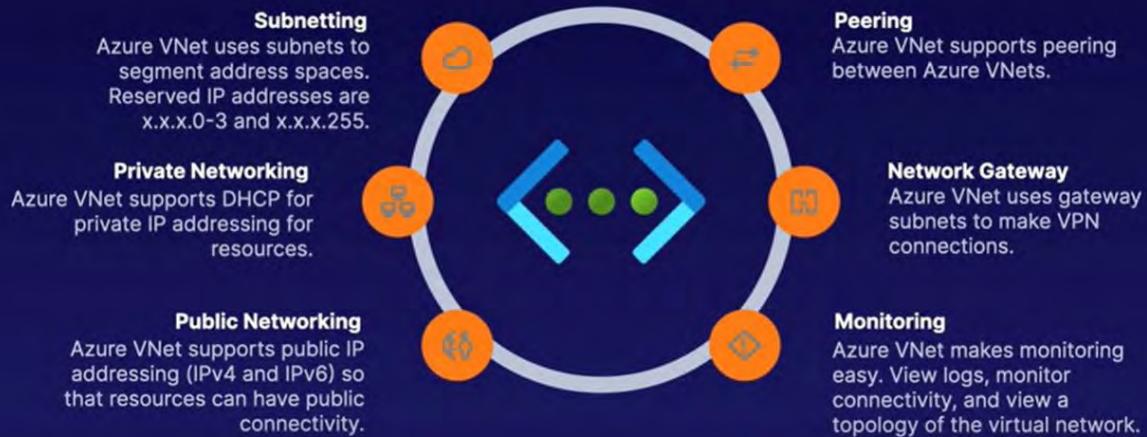
Determine what type of connectivity is needed: Internet, resource to resource, resource to service, etc.



Ips reservadas en subnets la 0,1,2,3 y 255

Virtual Network (VNet) Features

A CLOUD GU



El slash maximo para crear una vnet es 29

En los DNS puedes seleccionar el de default de Azure o uno custom:



Podemos modificar la ip de un equipo a estática o dinámica:

Public IP address settings

Public IP address

Disassociate Associate

Public IP address *

vnet-demo-vm-01-ip (20.97.11.151)

Create new

Private IP address settings

Virtual network/subnet

vnet-demo-01/default

Assignment

Dynamic Static

IP address

10.0.0.4



Key Takeaways



Nex
Crea



DNS and DHCP

Azure-provided DNS or custom DNS. For VNets, DHCP is built-in.



Network Integration

VNets are built for integration with one another, hybrid connectivity using VPNs, and ExpressRoute.



Supported Protocols

VNets support TCP, UDP, and ICMP protocols.



Things to know about subnets

There are certain conditions for the IP addresses in a virtual network when you apply segmentation with subnets.

- Each subnet contains a range of IP addresses that fall within the virtual network address space.
- The address range for a subnet must be unique within the address space for the virtual network.
- The range for one subnet can't overlap with other subnet IP address ranges in the same virtual network.
- The IP address space for a subnet must be specified by using CIDR notation.
- You can segment a virtual network into one or more subnets in the Azure portal. Characteristics about the IP addresses for the subnets are listed.

Name ↑↓	IPv4 ↑↓	IPv6 ↑↓	Available IPs. ↑↓	Delegated
subnet0	10.0.0.0/24	-	250	-
subnet1	10.0.1.0/24	-	251	-
subnet2	10.0.2.0/24	-	251	-
AzureBastionSubnet	10.0.30.0/27	-	27	-
GatewaySubnet	10.0.3.0/27	-	availability dependent on dynamic use	-

Reserved addresses

For each subnet, Azure reserves five IP addresses. The first four addresses and the last address are reserved.

Let's examine the reserved addresses in an IP address range of 192.168.1.0/24.

Reserved address	Reason
192.168.1.0	This value identifies the virtual network address.
192.168.1.1	Azure configures this address as the default gateway.
192.168.1.2 and 192.168.1.3	Azure maps these Azure DNS IP addresses to the virtual network space.
192.168.1.255	This value supplies the virtual network broadcast address.

Things to consider when using subnets

When you plan for adding subnet segments within your virtual network, there are several factors to consider. Review the following scenarios.

- Consider service requirements. Each service directly deployed into a virtual network has specific requirements for routing and the types of traffic that must be allowed into and out of associated subnets. A service might require or create their own subnet. There must be enough unallocated space to meet the service requirements. Suppose you connect a virtual network to an on-premises network by using Azure VPN Gateway. The virtual network must have a dedicated subnet for the gateway.
- Consider network virtual appliances. Azure routes network traffic between all subnets in a virtual network, by default. You can override Azure's default routing to prevent Azure routing between subnets. You can also override the default to route traffic between subnets through a network virtual appliance. If you require traffic between resources in the same virtual network to flow through a network virtual appliance, deploy the resources to different subnets.
- Consider service endpoints. You can limit access to Azure resources like an Azure storage account or Azure SQL database to specific subnets with a virtual network service endpoint. You can also deny access to the resources from the internet. You might create multiple subnets, and then enable a service endpoint for some subnets, but not others.
- Consider network security groups. You can associate zero or one network security group to each subnet in a virtual network. You can associate the same or a different network security group to each subnet. Each network security group contains rules that allow or deny traffic to and from sources and destinations.
- Consider private links. Azure Private Link provides private connectivity from a virtual network to Azure platform as a service (PaaS), customer-owned, or Microsoft partner services. Private Link simplifies the network architecture and secures the connection between endpoints in Azure. The service eliminates data exposure to the public internet.

Create virtual networks

✓ 100 XP

2 minutes

You can create new virtual networks at any time. You can also add virtual networks when you create a virtual machine.

Things to know about creating virtual networks

Review the following requirements for creating a virtual network.

- When you create a virtual network, you need to define the IP address space for the network.
- Plan to use an IP address space that's not already in use in your organization.
- The address space for the network can be either on-premises or in the cloud, but not both.
- You can't redefine the IP address space for a network after it's created. If you plan your address space for cloud-only virtual networks, you might later decide to connect an on-premises site.
- To create a virtual network, you need to define at least one subnet.
 - Each subnet contains a range of IP addresses that fall within the virtual network address space.
 - The address range for each subnet must be unique within the address space for the virtual network.
 - The range for one subnet can't overlap with other subnet IP address ranges in the same virtual network.
- You can create a virtual network in the Azure portal. Provide the Azure subscription, resource group, virtual network name, and service region for the network.
- Static IP addresses don't change and are best for certain situations, such as:
 - DNS name resolution, where a change in the IP address requires updating host records.
 - IP address-based security models that require apps or services to have a static IP address.
 - TLS/SSL certificates linked to an IP address.
 - Firewall rules that allow or deny traffic by using IP address ranges.
 - Role-based virtual machines such as Domain Controllers and DNS servers.

A public IP address resource can be associated with virtual machine network interfaces, internet-facing load balancers, VPN gateways, and application gateways. You can associate your resource with both dynamic and static public IP addresses.

Things to consider when associating public IP addresses

The following table summarizes how you can associate public IP addresses for different types of resources.

Resource	Public IP address association	Dynamic IP address	Static IP address
Virtual machine	NIC	Yes	Yes
Load balancer	Front-end configuration	Yes	Yes
VPN gateway	VPN gateway IP configuration	Yes	Yes *
Application gateway	Front-end configuration	Yes	Yes *

* Static IP addresses are available on certain SKUs only.

Public IP address SKUs

When you create a public IP address, you select the Basic or Standard SKU. Your SKU choice affects the IP assignment method, security, available resources, and redundancy options.

The following table summarizes the differences between the SKU types for public IP addresses.

Feature	Basic SKU	Standard SKU
IP assignment	Static or Dynamic	Static
Security	Open by default	Secure by default, closed to inbound traffic
Resources	Network interfaces, VPN gateways, Application gateways, and internet-facing load balancers	Network interfaces or public standard load balancers
Redundancy	Not zone redundant	Zone redundant by default

Deploying network resources



Types of IPs



Private IPs

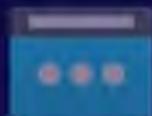
Statically or dynamically assigned addresses that allow private connectivity between resources.



Public IPs

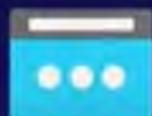
Statically or dynamically assigned addresses that allow public connectivity from the internet to a resource.

Public IP SKUs



Basic SKU

Statically or dynamically assignable PIP that is accessible by default and requires an NSG to restrict traffic. Does not support availability zone deployments.



Standard SKU

Statically assignable PIP that is not accessible by default and requires an NSG to allow traffic. Supports availability zone deployments.

Todas las configuraciones se hacen en la NIC virtual

Network Interface Card (NIC)	
	IP Configurations
	Private IP: 10.0.0.4
	Public IP: X.X.X.X

Para crear una Ip publica la creamos primero y luego en la nic la asociamos, pero deben estar en la misma región

Things to consider when associating private IP addresses

The following table summarizes how you can associate private IP addresses for different types of resources.

Resource	Private IP address association	Dynamic IP address	Static IP address
Virtual machine	NIC	Yes	Yes
Internal load balancer	Front-end configuration	Yes	Yes
Application gateway	Front-end configuration	Yes	Yes

Private IP address assignment

A private IP address is allocated from the address range of the virtual network subnet that a resource is deployed in. There are two options: dynamic and static.

- Dynamic: Azure assigns the next available unassigned or unreserved IP address in the subnet's address range.
Dynamic assignment is the default allocation method.

Suppose addresses 10.0.0.4 through 10.0.0.9 are already assigned to other resources. In this case, Azure assigns the address 10.0.0.10 to a new resource.

- Static: You select and assign any unassigned or unreserved IP address in the subnet's address range.

Suppose a subnet's address range is 10.0.0.0/16, and addresses 10.0.0.4 through 10.0.0.9 are already assigned to other resources. In this scenario, you can assign any address between 10.0.0.10 and 10.0.255.254.

- The Sales department has a subnet with an address range of 10.3.0.0/16.
- The infrastructure team has firewall rules to deny traffic based on IP address ranges.
- You're examining how to use Azure Virtual Network to enable communication between resources within the company network and in the cloud.

Answer the following questions

Choose the best response for each of the following questions. Then select Check your answers.

1. For the Sale department subnet range, which IP address can be dynamically assigned? *

- 10.3.0.2
- 10.3.255.255
- 10.3.255.254

✓ Correct. Any address in the range 10.3.0.4 through 10.3.255.254 is available for assignment.

2. What feature can support the denial of traffic based on the IP address range? *

- Statically assigned IP addresses
- ✓ Correct. In this situation, use statically assigned IP addresses to avoid having to change the firewall rules.
- Dynamically assigned IP addresses
- IP addresses in the reserved range

✗ Incorrect. IP addresses in the reserved range can't be used.

3. Which of the following statements about Azure Virtual Network is correct? *

- Outbound communication with the internet must be configured for each resource on the virtual network.
 - ✗ Incorrect. All resources in a virtual network can communicate outbound to the internet, by default.
 - Azure Virtual Network enables communication between Azure resources.
- ✓ Correct. Azure Virtual Network connects Azure resources including virtual machines, the Azure App Service Environment, Azure Kubernetes Service (AKS), and Azure Virtual Machine Scale Sets. You can use service endpoints to connect to other Azure resource types, such as Azure SQL databases and storage accounts.
- Azure virtual networks can't be configured to communicate with on-premises resources.

Routes = Paths for Connectivity

Routes are paths through which traffic can flow.

For example, a route allowing virtual machines to communicate with the internet outbound.

Routing Types

System Routes

Default routes built-in to virtual networks that cannot be modified.

Custom Routes

User-defined routes or border gateway protocol (BGP) routes that override system routes.

BGP Route

Routes that are exchanged between integrated networks.

For example, hybrid networks or VNet peering scenarios.

Para modificar estas rutas nos vamos a effective routes dentro de la nic

The screenshot shows the Azure portal interface for managing network interfaces. The left sidebar has a tree view with items like Network security group, Properties, Locks, Monitoring, Alerts, Metrics, Diagnostic settings, Automation, Tasks (preview), Export template, Support + troubleshooting, Effective security rules, and Effective routes. The Effective routes item is selected and highlighted in blue. The main content area is titled 'rt-demo-vm-01VMNic | Effective routes'. It shows a table of 'Effective routes' with the following data:

Source	State	Address Prefixes	Next Hop Type
Default	Active	10.0.0.0/16	Virtual network
Default	Active	0.0.0.0/0	Internet
Default	Active	10.0.0.0/8	None
Default	Active	100.64.0.0/10	None
Default	Active	192.168.0.0/16	None
Default	Active	25.33.80.0/20	None
Default	Active	25.41.3.0/25	None

En route tables creamos nuevas tablas de routeo.

Las reglas de usuario se sobreponen a las que vienen por default.

Custom> BGP > System

Network Security Groups

NSGs Control the Flow of Traffic

A network security group (NSG) controls the traffic flowing through a virtual network. This is done so by:

- Creating rules that define what is allowed/denied
- Controlling security at the subnet or NIC network layers
- Specifying rule priority

Defining NSGs



Filter Traffic

Determining what traffic will be allowed or denied inbound and outbound.



Rules

Evaluating default rules that cannot be deleted and user-defined rules that can be created.



Priority

Specifying priority to order the precedence of rules. The lower the number, the higher the priority.

Priority ↑	Name ↑↓	Port ↑↓	Protocol ↑↓	Source ↑↓	Destination ↑↓	Action ↑↓
✓ Inbound Security Rules						
65000	AllowVnetInbound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalanc...	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInbound	Any	Any	Any	Any	Deny
✓ Outbound Security Rules						
65000	AllowVnetOutbound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutbound	Any	Any	Any	Internet	Allow
65500	DenyAllOutbound	Any	Any	Any	Any	Deny

Defining NSGs



Association

An NSG has no effect unless associated to either a subnet or network interface card (NIC).



Precedence

"Let the traffic guide you" into evaluating which rules are processed. Once a rule is matched, no other rule is read.

Example:

Priority ↑	Name ↑↓	Port ↑↓	Protocol ↑↓	Source ↑↓	Destination ↑↓	Action ↑↓
✓ Inbound Security Rules						
100	⚠ allow_ssh	22	TCP	Any	Any	Allow
65000	AllowVnetInbound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowAzureLoadBalanc...	Any	Any	AzureLoadBalancer	Any	Allow
65500	DenyAllInbound	Any	Any	Any	Any	Deny
✓ Outbound Security Rules						
65000	AllowVnetOutbound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutbound	Any	Any	Any	Internet	Allow
65500	DenyAllOutbound	Any	Any	Any	Any	Deny

Las user priority numbers pueden ser numero del 100-4096



Follow the Traffic

Evaluate rules by following the traffic. Inbound traffic checks the subnet, then the NIC for NSGs. Outbound traffic checks the NIC, then the subnet for NSGs. Intra-net traffic is affected.

Podemos meter Vms en un application security group y ese group llamarlo en la network security rule para aplicar esa regla en todos los servers dentro de ese app group

Things to know about network security groups

Let's look at the characteristics of network security groups.

- A network security group contains a list of security rules that allow or deny inbound or outbound network traffic.
- A network security group can be associated to a subnet or a network interface.
- A network security group can be associated multiple times.
- You create a network security group and define security rules in the Azure portal.

Network security groups are defined for your virtual machines in the Azure portal. The Overview page for a virtual machine provides information about the associated network security groups. You can see details such as the assigned subnets, assigned network interfaces, and the defined security rules.

The screenshot shows the Azure portal's 'Overview' page for a Network Security Group named 'nsg0'. The main pane displays the following details:

- Resource group (change) : rg0
- Location : East US
- Subscription (change) :
- Subscription ID:
- Tags (change) : Click here (add tags)

On the left, there is a sidebar with navigation links: Overview, Activity log, Access control (IAM), Tags, and Diagnose and solve problems. At the top, there are buttons for Move, Delete, and Refresh, along with a search bar and a 'Did you mean?' dropdown.

Network security groups and subnets

You can assign network security groups to a subnet and create a protected screened subnet (also referred to as a demilitarized zone or DMZ). A DMZ acts as a buffer between resources within your virtual network and the internet.

- Use the network security group to restrict traffic flow to all machines that reside within the subnet.
- Each subnet can have a maximum of one associated network security group.

Network security groups and network interfaces

You can assign network security groups to a network interface card (NIC).

- Define network security group rules to control all traffic that flows through a NIC.
- Each network interface that exists in a subnet can have zero, or one, associated network security groups.

Things to know about security rules

Let's review the characteristics of security rules in network security groups.

- Azure creates several default security rules within each network security group, including inbound traffic and outbound traffic. Examples of default rules include DenyAllInbound traffic and AllowInternetOutbound traffic.
- Azure creates the default security rules in each network security group that you create.
- You can add more security rules to a network security group by specifying conditions for any of the following settings:
 - Name
 - Priority
 - Port
 - Protocol (Any, TCP, UDP)
 - Source (Any, IP addresses, Service tag)
 - Destination (Any, IP addresses, Virtual network)
 - Action (Allow or Deny)
- Each security rule is assigned a Priority value. All security rules for a network security group are processed in priority order. When a rule has a low Priority value, the rule has a higher priority or precedence in terms of order processing.
- You can't remove the default security rules.
- You can override a default security rule by creating another security rule that has a higher Priority setting for your network security group.

Inbound traffic rules

Azure defines three default inbound security rules for your network security group. These rules deny all inbound traffic except traffic from your virtual network and Azure load balancers. The following image shows the default inbound security rules for a network security group in the Azure portal.



PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	<input checked="" type="checkbox"/> Allow
65001	AllowAzureLoadBalancerInBound	Any	Any	AzureLoadBalancer	Any	<input checked="" type="checkbox"/> Allow
65500	DenyAllInBound	Any	Any	Any	Any	<input checked="" type="checkbox"/> Deny

Outbound traffic rules

Azure defines three default outbound security rules for your network security group. These rules only allow **outbound traffic** to the internet and your **virtual network**. The following image shows the default outbound security rules for a network security group in the Azure portal.

PRIORITY	NAME	PORT	PROTOCOL	SOURCE	DESTINATION	ACTION
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	Allow
65500	DenyAllOutBound	Any	Any	Any	Any	Deny

Determine network security group effective rules

✓ 100 XP

5 minutes

Each network security group and its defined security rules are evaluated independently. Azure processes the conditions in each rule defined for each virtual machine in your configuration.

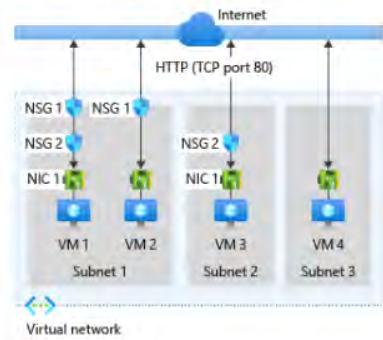
- For inbound traffic, Azure first processes **network security group security rules** for any associated subnets and then any associated network interfaces.
- For outbound traffic, the process is reversed. Azure first evaluates **network security group security rules** for any associated network interfaces followed by any associated subnets.
- For both the inbound and outbound evaluation process, Azure also checks how to apply the rules for intra-subnet traffic.

How Azure ends up applying your defined security rules for a virtual machine determines the overall **effectiveness** of your rules.

Things to know about effective security rules

Let's explore how network security group rules are defined and processed within a virtual network to yield the effective rules.

Consider the following virtual network configuration that shows network security groups (NSGs) controlling traffic to virtual machines (VMs). The configuration requires security rules to manage network traffic to and from the internet over TCP port 80 via the network interface.



In this virtual network configuration, there are three subnets. Subnet 1 contains two virtual machines: VM 1 and VM 2. Subnet 2 and Subnet 3 each contain one virtual machine: VM 3 and VM 4, respectively. Each VM has a network interface card (NIC).

Azure evaluates each NSG configuration to determine the effective security rules:

Evaluation	Subnet NSG	NIC NSG	Inbound rules	Outbound rules
VM 1	Subnet 1 NSG 1	NIC NSG 2	NSG 1 subnet rules have precedence over NSG 2 NIC rules	NSG 2 NIC rules have precedence over NSG 1 subnet rules
VM 2	Subnet 1 NSG 1	NIC none	NSG 1 subnet rules apply to both subnet and NIC	Azure default rules apply to NIC and NSG 1 subnet rules apply to subnet only
VM 3	Subnet 2 none	NIC NSG 2	Azure default rules apply to subnet and NSG 2 rules apply to NIC	NSG 2 NIC rules apply to NIC and subnet
VM 4	Subnet 3 none	NIC none	Azure default rules apply to both subnet and NIC and all inbound traffic is allowed	Azure default rules apply to both subnet and NIC and all outbound traffic is allowed

Things to consider when creating effective rules

Review the following considerations regarding creating effective security rules for machines in your virtual network.

- Consider allowing all traffic. If you place your virtual machine within a subnet or utilize a network interface, you don't have to associate the subnet or NIC with a network security group. This approach allows all network traffic through the subnet or NIC according to the default Azure security rules. If you're not concerned about controlling traffic to your resource at a specific level, then don't associate your resource at that level to a network security group.
- Consider importance of allow rules. When you create a network security group, you must define an allow rule for both the subnet and network interface in the group to ensure traffic can get through. If you have a subnet or NIC in your network security group, you must define an allow rule at each level. Otherwise, the traffic is denied for any level that doesn't provide an allow rule definition.
- Consider intra-subnet traffic. The security rules for a network security group that's associated to a subnet can affect traffic between all virtual machines in the subnet. By default, Azure allows virtual machines in the same subnet to send traffic to each other (referred to as *intra-subnet traffic*). You can prohibit intra-subnet traffic by defining a rule in the network security group to deny all inbound and outbound traffic. This rule prevents all virtual machines in your subnet from communicating with each other.
- Consider rule priority. The security rules for a network security group are processed in priority order. To ensure a particular security rule is always processed, assign the lowest possible priority value to the rule. It's a good practice to leave gaps in your priority numbering, such as 100, 200, 300, and so. The gaps in the numbering allow you to add new rules without having to edit existing rules.

Things to know about using application security groups

Application security groups work in the same way as network security groups, but they provide an application-centric way of looking at your infrastructure. You join your virtual machines to an application security group. Then you use the application security group as a source or destination in the network security group rules.

Let's examine how to implement application security groups by creating a configuration for an online retailer. In our example scenario, we need to control network traffic to virtual machines in application security groups.



Things to consider when using application security groups

There are several advantages to implementing application security groups in your virtual networks.

- Consider IP address maintenance.** When you control network traffic by using application security groups, you don't need to configure inbound and outbound traffic for specific IP addresses. If you have many virtual machines in your configuration, it can be difficult to specify all of the affected IP addresses. As you maintain your configuration, the number of your servers can change. These changes can require you to modify how you support different IP addresses in your security rules.
- Consider no subnets.** By organizing your virtual machines into application security groups, you don't need to also distribute your servers across specific subnets. You can arrange your servers by application and purpose to achieve logical groupings.
- Consider simplified rules.** Application security groups help to eliminate the need for multiple rule sets. You don't need to create a separate rule for each virtual machine. You can dynamically apply new rules to designated application security groups. New security rules are automatically applied to all the virtual machines in the specified application security group.
- Consider workload support.** A configuration that implements application security groups is easy to maintain and understand because the organization is based on workload usage. Application security groups provide logical arrangements for your applications, services, data storage, and workloads.

Knowledge check

✓ 200 XP

3 minutes

Your company is migrating several sites to Azure. You're responsible for implementing network security groups and designing effective security rules to control network traffic. You need to ensure that virtual machine networking and Azure services networking are both secure.

- The infrastructure team has two network security group security rules for inbound traffic to the back-end web servers. There's an allow rule with a priority of 200, and a deny rule with a priority of 150.
- The IT team wants to apply new and pre-existing Azure service tags for the virtual machine IP addresses.
- You're exploring how to use default rules to apply security to inbound traffic from virtual machines within your virtual network.

Answer the following questions

Choose the best response for each of the following questions. Then select Check your answers.

1. Which of the security rules defined by the infrastructure team takes precedence? *

- The allow rule takes precedence.
- The deny rule takes precedence.
- Correct. The deny rule takes precedence because it's processed first. The rule with priority 150 is processed before the rule with priority 200.
- The rule that was created first takes precedence.

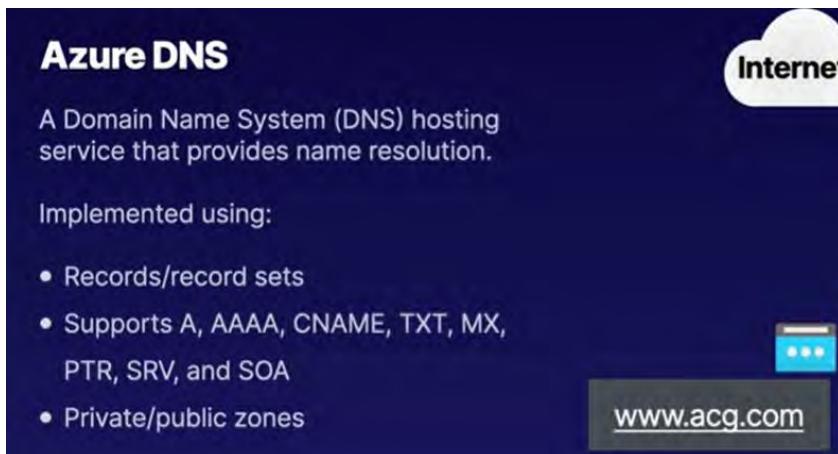
2. How would you define a default inbound security rule? *

- Allow inbound coming from a virtual machine in another virtual network.
- Allow traffic from any external source to any of the virtual machines.
- Allow inbound coming from any virtual machine to any other virtual machine within the virtual network.
- Correct. By default, inbound security rules allow traffic from any virtual machine to any other virtual machine within the virtual network.

3. What's a valid service tag for network security group rules? *

- VirtualNetwork.
- Correct. `VirtualNetwork` is a valid service tag. Service tags represent a group of IP addresses. Other service tags are `Internet`, `SQL`, `Storage`, `AzureLoadBalancer`, and `AzureTrafficManager`.
- VPN Gateway.
- `VirtualNetwork`

Using Azure DNS



Podemos asociar un nombre a un resource y no necesariamente a una IP

Add record set X

thecloudchase.com

Name
 ✓

Type
A – Alias record to IPv4 address ^

A – Alias record to IPv4 address ▼

AAAA – Alias record to IPv6 address

CAA – Certificate Authorities to authorize certificates

CNAME – Link your subdomain to another record

MX – Mail eXchange records

NS – Name Server records

SRV – Service records

TXT – Text record type

PTR – Pointer record type

Para Private DNS zones solo podemos linkear networks que hayan sido creadas por Resource manager deployment model . Las creadas con el Classic deployment no son soportadas

Considerations

Features:

- Role-Based Access Control (RBAC)
- Activity logs
- Resource locking
- Private DNS zone

Identify domains and custom domains

✓ 100 XP

2 minutes

Azure DNS enables you to host your DNS domains in Azure and access name resolution for your domains by using Microsoft Azure infrastructure. You can configure and manage your custom domains with Azure DNS in the Azure portal. By accessing your domains in Azure, you can use your same credentials, support agreements, and billing preferences as for your other Azure services.

Before you begin using Azure DNS to host DNS records for your domains, there are a few important concepts to review.

Things to know about domain names in Azure

Things to know about domain names in Azure

Let's examine how an *initial domain name* and *custom domain names* are implemented in Azure.

- When you create an Azure subscription, Azure automatically creates an Azure Active Directory (Azure AD) domain for your subscription.

Note

You must be a global administrator to perform domain management tasks. The global administrator is the user who created the subscription.

- Azure applies an initial domain name to your initial domain instance.
- The initial domain name follows the form <Your Domain Name> followed by .onmicrosoft.com. For example, `yourdomainname.onmicrosoft.com`.
- The purpose of a custom domain name is to provide a simplified form of your domain name to support specific users or tasks.

Organizations commonly implement custom domain names to enable users to access their domain by using credentials they're familiar with.

Consider the Azure Administrator Incorporated Azure AD domain. Azure creates the initial domain name for the Azure AD instance as `azureadmininc.onmicrosoft.com`. A custom domain name for the instance could be `azureadmininc.org`.



- The initial domain name is intended to be used until your custom domain name is *verified*.
- Before a custom domain name can be used by Azure AD, the custom domain name must be added to your directory and verified.
- The initial domain name can't be changed or deleted, but you can add a routable custom domain name that you control.
- In Azure AD, domain names must be *globally unique*. When one Azure AD directory has verified a specific domain name, other Azure AD directories can't use that same domain name.

Verify custom domain names

◀ 100 XP

2 minutes

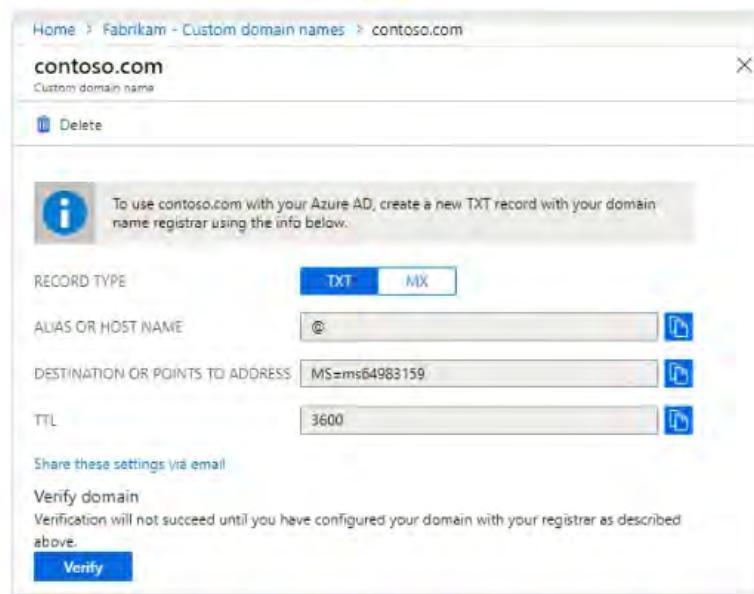
When an administrator adds a custom domain name to an Azure Active Directory instance, the custom domain name is initially in an *unverified* state. Azure AD won't allow any directory resources to use a custom domain name that's unverified.

Before you can use a custom domain name for your Azure AD instance, your custom domain name must be *verified*.

How to verify your custom domain name

After you add a custom domain name for your Azure AD instance in the Azure portal, you must verify ownership of your custom domain name.

You initiate the verification process by adding a DNS record for your custom domain name. The DNS record type can be MX or TXT, as shown in the following image:



The MX (or Mail exchange) record lists mail exchange servers that accept email for your domain. The TXT (or Text) record indicates human-readable text or machine-readable data about your domain. These record types are defined in RFC 1035⁴.

After you add a DNS record to your custom domain name, Azure queries the DNS domain for the presence of the DNS record.

ⓘ Note

The Azure verification process can take several minutes or hours.

After Azure verifies the presence of the DNS record for your custom domain name, Azure adds your new custom domain name to your subscription for the Azure AD instance.

Azure DNS provides a reliable, secure DNS service to manage and resolve domain names in a virtual network without needing to add a custom DNS solution.

An Azure DNS zone hosts the DNS records for a domain. To begin hosting your domain in Azure DNS, you need to create a DNS zone for your domain name. Each DNS record for your domain is then created inside your DNS zone.

Things to know about DNS zones

You can add a DNS zone in the Azure portal, as shown in the following image. Several configuration settings are required to create a DNS zone. In the portal, you specify the DNS zone name, number of records, resource group, zone location, associated subscription, and DNS name servers.

The screenshot shows the 'Create DNS zone' wizard in the Azure portal. The 'Basics' tab is selected. The 'Project details' section includes fields for 'Subscription' (Visual Studio Enterprise Subscription) and 'Resource group' (a dropdown with 'Create new'). The 'Instance details' section includes a checkbox for 'This zone is a child of an existing zone already hosted in Azure DNS' and fields for 'Name' and 'Resource group location'. At the bottom, there are buttons for 'Review + create', 'Previous', 'Next: Tags >', and 'Download a template for automation'.

Take a moment to review some important characteristics about DNS zones.

- Within a resource group, the name of a DNS zone must be unique. By providing a unique name when you create a new DNS zone, Azure ensures that the DNS zone doesn't already exist in the resource group.
- Multiple DNS zones can have the same name, but the DNS zones must exist in different resource groups or in different Azure subscriptions.
- When multiple DNS zones share the same name, each DNS zone instance is assigned to a different DNS name server address.
- The Root/Parent domain is registered at the registrar and then pointed to Azure DNS.
- Child domains are registered directly in Azure DNS.

Tip:

You don't have to own a domain name to create a DNS zone with that domain name in Azure DNS. However, you do need to own the domain to configure the domain.

Delegate DNS domains

100 XP

3 minutes

To delegate your domain to Azure DNS, you need to identify the DNS name servers for your DNS zone. Each time a DNS zone is created, Azure DNS allocates DNS name servers from a pool. After the DNS name servers are assigned, Azure DNS automatically creates authoritative NS (or Name server) records in your DNS zone.

The delegation process for your domain involves several steps:

1. Identify your DNS name servers
2. Update your parent domain
3. Delegate subdomains (optional)

How to find your DNS name servers

The easiest way to find the DNS name servers assigned to your DNS zone is through the Azure portal.

Let's take another look at our sample Azure Administrator Incorporated Azure AD domain. In a previous unit, we defined a custom domain name for the sample instance as `azureadmin101.org`. In the Azure portal, we can examine the custom domain and find that Azure assigned four DNS name servers to the DNS zone for the domain: `ns1-02.azure-dns.com`, `ns2-02.azure-dns.net`, `ns3-02.azure-dns.org`, and `ns4-02.azure-dns.info`.

The screenshot shows the Azure portal interface for managing a DNS zone named `contosotest.com`. The left sidebar lists navigation options like Overview, Activity log, Access control (IAM), Tags, and more. The main area is titled "contosotest.com" and "DNS zone". It includes a search bar, a toolbar with "Record set", "Child zone", and "Move" buttons, and a "Essentials" summary section. The "Essentials" section provides details about the Resource group (`azurednsrg`), Subscription (`change`), and Subscription ID. Below this, a list of "Name servers" is shown, each with its corresponding FQDN: `ns1-04.azure-dns.com`, `ns2-04.azure-dns.net`, `ns3-04.azure-dns.org`, and `ns4-04.azure-dns.info`. At the bottom of the page, there are sections for "Properties" and "Tags (change)".

How to update your parent domain

After your DNS zone is created, and you can identify your DNS name servers, you need to update your parent domain.

Each registrar has their own DNS management tools to manage the DNS name server records for a domain. The term *registrar* refers to the third-party domain registrar, which is the company where you registered your domain.

Here's a basic process you can follow to update your parent domain information with your registrar:

1. Go to your registrar's DNS management page.
2. Find the existing `NS` records for your parent domain.
3. Replace the existing `NS` records with the `NS` records created for your domain by Azure DNS.

Things to consider when working with NS records

There are several important considerations to keep in mind when working with `NS` records and name servers for a DNS zone.

- When you copy an `NS` record (a DNS name server address), be sure to include the trailing period (.) at the end of the address. The trailing period indicates the end of a fully qualified domain name, such as `ns1-02.azure-dns.com.` and `ns3-02.azure-dns.org..`
- To delegate your domain to Azure DNS, you must use the exact names of the DNS name servers as created by Azure DNS.
- We recommend that you always copy all DNS name server `NS` records for your domain to the parent domain, regardless of the actual domain name. In our sample scenario, suppose we don't expect traffic on the `ns4-02.azure-dns.info.` DNS name server. Although we don't expect traffic on this DNS name server address, the best practice is to also copy this `NS` record to the parent domain with the other name server addresses.

How to delegate subdomains

You can delegate a subdomain for your domain in Azure DNS by setting up a separate child DNS zone.

Let's consider our sample Azure Administrator Incorporated Azure AD domain. We created a custom domain name for the instance as `azureadmininc.org`. We can configure a separate child DNS zone for the custom domain to support partners of the organization, such as `partners.azureadmininc.org`.

The configuration steps for delegating a child DNS zone are similar to the typical delegation process. The key difference is you don't work with your registrar to delegate a subdomain. You delegate the child DNS zone in the Azure portal.

Here are the steps to delegate a subdomain:

1. Go to the parent DNS zone for your domain in the Azure portal.
2. Find the existing `NS` records for your parent domain.
3. Create new `NS` records for your child DNS zone (subdomain).

ⓘ Note

The parent and child DNS zones can be in the same or different resource group.

In our example, notice that the `NS` record server name in child DNS zone is the same name as for the parent DNS zone, `azureadmininc.com`. The one difference that identifies the subdomain is the addition of the keyword `partners` with the separating period (`.`).

Add DNS record sets

✓ 100 XP

2 minutes

It's important to understand the difference between DNS record sets and individual DNS records. A DNS record set (also known as a *resource record set*) is a collection of records in a DNS zone.

You define record sets in the Azure portal. The configuration settings depend on the record type for the set to create.

Suppose you choose to create a set of A records (or *Address record*) to identify IP addresses associated with your domain. To create the A records, you need to provide the TTL (time to live) and the IP addresses. The TTL value specifies how long each record is cached by clients.

The screenshot shows the Azure portal interface for managing Private DNS zones. On the left, there's a navigation bar with 'Home > Private DNS zones >'. Below it is a list of zones, with 'privatelink.servicebus.windows.net' selected. The main area is titled 'Add record set' and shows a dialog for creating an A record. The 'Name' field contains '.privatelink.servicebus.windows.net'. The 'Type' dropdown is set to 'A – Address record'. Under 'TTL *', the value is '1' and the unit is 'Hours'. In the 'IP address' field, the value '0.0.0.0' is entered. At the bottom right of the dialog is a large green 'Create' button.

Things to know about DNS record sets

Let's examine some characteristics of DNS record sets.

- All records in a DNS record set must have the same name and the same record type.

Consider the following example where we have two records in a record set. All records have the same name, `www.contoso.com.`. All records have the same record type, `A`. Each record in the set has a different value. In this case, each record provides a different IP address.

Console					Copy
www.contoso.com.	3600	IN	A	134.170.185.46	
www.contoso.com.	3600	IN	A	134.170.188.221	

- A DNS record set can't contain two identical records.
- A record set of type `CNAME` can contain only one record.

A `CNAME` record (or *Canonical name record*) provides an alias of one domain name to another. This record is used to provide another name for your domain. The DNS `lookup` operation tries to find your domain by retrying the `lookup` with the other name specified in the `CNAME` record.

- You can create a record set that doesn't have any records. This set is called an *empty record set*.
- If you have an empty record set for your domain, this set doesn't appear on your Azure DNS name servers.

Things to know about Azure Private DNS benefits

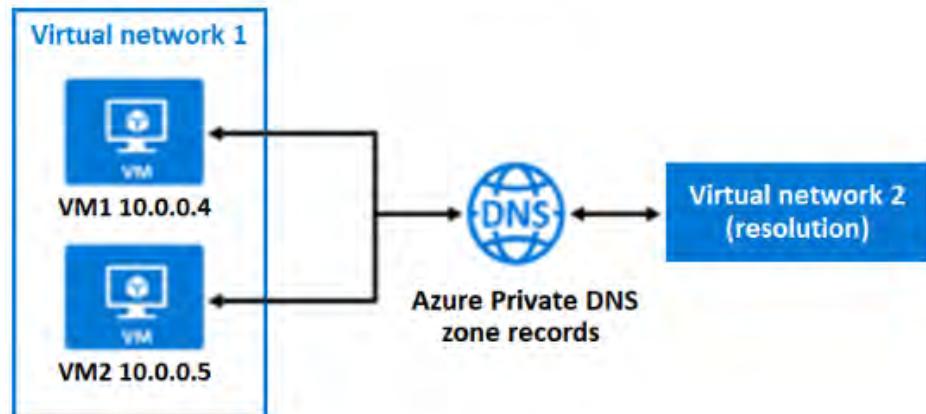
There are many benefits to implementing Azure Private DNS for your domain.

Benefit	Description
No custom DNS solution required	Previously, many customers created custom DNS solutions to manage DNS zones in their virtual network. You can now perform DNS zone management by using the native Azure infrastructure. Azure Private DNS removes the burden of creating and managing custom DNS solutions.
Support for common DNS records types	Azure Private DNS supports all common DNS record types, including A, AAAA, CNAME, MX, PTR, SOA, SRV, and TXT.
Automatic hostname record management	Along with hosting your custom DNS records, Azure Private DNS automatically maintains hostname records for the virtual machines in the specified virtual networks. In this scenario, you can optimize the domain names you use without needing to create custom DNS solutions or modify applications.
Hostname resolution between virtual networks	Unlike Azure-provided host names, Azure Private DNS zones can be shared between virtual networks. This capability simplifies cross-network and service-discovery scenarios, such as virtual network peering.
Familiar tools and user experience	To reduce the learning curve, Azure Private DNS uses well-established Azure DNS tools, including PowerShell, Azure Resource Manager (ARM) templates, and the REST API.
Split-horizon DNS support	With Azure Private DNS, you can create zones with the same name that resolve to different answers from within a virtual network and from the public internet. A typical scenario for a split-horizon DNS is to provide a dedicated version of a service for use inside your virtual network.
Azure region support	Azure Private DNS zones are available in all Azure regions in the Azure public cloud.

In the next section, we'll review some common implementation scenarios for Azure Private DNS.

Scenario 1: Name resolution scoped to a single virtual network

The first scenario consists of virtual networks and resources in Azure that include virtual machines. The resources need to be resolved from within the virtual network by using a specific domain name (or DNS zone). The name resolution needs to be private and not accessible from the internet. The scenario requires that Azure should automatically register the virtual machines within the virtual network into the DNS zone.



Let's examine the details of this scenario:

- Virtual network 1 contains two virtual machines: VM1 and VM2. VM1 and VM2 each have a private IP address.
- When an Azure Private DNS zone address is created (such as `contoso.lab`) and linked to Virtual network 1, Azure DNS automatically creates two A records in the DNS zone if Auto registration is enabled in the link configuration.
- In this scenario, Azure DNS uses only Virtual network 2 to resolve domain name (or DNS zone) queries.

Azure DNS queries from VM1 in Virtual network 1 to resolve the `VM2.contoso.lab` address receive an Azure DNS response that contains the private IP address of VM2 (10.0.0.5).

- A reverse DNS query (PTR) for the private IP address of VM1 (10.0.0.4) issued from VM2 receive an Azure DNS response that contains the FQDN of VM1, as expected.

}

Scenario 2: Name resolution for multiple networks

The second scenario involves name resolution across multiple virtual networks, which is probably the most common usage for Azure Private DNS zones. This scenario consists of two virtual networks. One network is focused on registration for Azure Private DNS zone records and the other supports name resolution.



Here are the details of this configuration:

- Virtual network 1 is designated for *registration*. Virtual network 2 is designated for *name resolution*.
- The design strategy is for both virtual networks to share the common DNS zone address, `contoso.lab`.
- The resolution and registration virtual networks are linked to the common DNS zone.
- Azure Private DNS zone records for virtual machines in Virtual network 1 (registration) are created automatically.
- For virtual machines in Virtual network 2 (resolution), Azure Private DNS zone records can be created manually.
- In this scenario, Azure DNS uses both virtual networks to resolve domain name queries.

An Azure DNS query from a virtual machine in Virtual network 2 (resolution) for a virtual machine in Virtual network 1 (registration) receives an Azure DNS response containing the private IP address of the virtual machine.

- Reverse DNS queries are scoped to the same virtual network.
 - A reverse DNS (PTR) query from a virtual machine in Virtual network 2 (resolution) for a virtual machine in Virtual network 1 (registration) receives an Azure DNS response containing the `NXDOMAIN` of the virtual machine. `NXDOMAIN` is an error message that indicates the queried domain doesn't exist.
 - A reverse DNS (PTR) query from a virtual machine in Virtual network 1 (registration) for a virtual machine also in Virtual network 1 receives the FQDN for the virtual machine.

1. Which summary best describes the main purpose of Azure DNS? *

- Azure DNS manages the security and access to your website.
- Azure DNS manages and hosts the registered domain for a website and its associated records.

✓ Correct. Azure DNS hosts the registered domains. Administrators can control and configure domain records like A, CNAME, and MX, and set up alias records.

- Azure DNS registers new domain names, so there's no need to use a domain registrar.

2. What type of DNS record can map one or more IP addresses against a single domain? *

- CNAME
- SOA
- A or AAAA

✓ Correct. The A or AAAA record maps an IP address to a domain. Multiple IP addresses are known as a *record set*.

3. Azure Private DNS supports which of the following scenarios? *

- Organizations manage and resolve domain names in a virtual network without adding a custom DNS solution.
- ✓ Correct. Azure Private DNS manages and resolves domain names in a virtual network without adding a custom DNS solution.
- Organizations manage and resolve domain names in a virtual network by adding a custom DNS solution.

✗ Incorrect. Azure Private DNS doesn't require adding a custom DNS solution.

- Organizations manage domain names in other organizations.

What is Azure DNS?

200 XP

7 minutes

Azure DNS is a hosting service for DNS domains that provides name resolution by using Microsoft Azure infrastructure.

In this unit, you'll learn what DNS is and how it works. You will also learn about Azure DNS, and why you would use it.

What is DNS?

DNS, or the Domain Name System, is a protocol within the TCP/IP standard. DNS serves an essential role of translating the human-readable domain names, for example: www.wideworldimports.com, into a known IP address. IP addresses enable computers and network devices to identify and route requests between themselves.

DNS uses a global directory hosted on servers around the world. Microsoft is part of that network that provides a DNS service through Azure DNS.

A DNS server is also known as a DNS name server, or just a name server.

How does DNS work?

A DNS server carries out one of two primary functions:

- Maintains a local cache of recently accessed or used domain names and their IP addresses. This cache provides a faster response to a local domain lookup request. If the DNS server can't find the requested domain, it passes the request to another DNS server. This process repeats at each DNS server until either a match is made or the search times out.
- Maintains the key-value pair database of IP addresses and any host or subdomain over which the DNS server has authority. This function is often associated with mail, web, and other internet domain services.

DNS server assignment

In order for a computer, server, or other network-enabled device to access web-based resources, it must reference a DNS server.

When you connect by using your on-premises network, the DNS settings come from your server. When you connect by using an external location, like a hotel, the DNS settings come from the internet service provider (ISP).

Domain lookup requests

Here's a simplified overview of the process a DNS server uses when it resolves a domain name lookup request:

- Checks to see if the domain name is stored in the short-term cache. If so, the DNS server resolves the domain request.
- If the domain isn't in the cache, it contacts one or more DNS servers on the web to see if they have a match. When a match is found, the DNS server updates the local cache and resolves the request.
- If the domain isn't found after a reasonable number of DNS checks, the DNS server responds with a *domain cannot be found* error.

IPv4 and IPv6

Every computer, server, or network-enabled device on your network has an IP address. An IP address is unique within your domain. There are two standards of IP address: IPv4 and IPv6.

- IPv4 is composed of four sets of numbers, in the range 0 to 255, each separated by a dot. Example: 127.0.0.1. Today, IPv4 is the most commonly used standard. Yet, with the increase in IoT devices, the IPv4 standard will eventually be unable to keep up.
- IPv6 is a relatively new standard and will eventually replace IPv4. It's made up of eight groups of hexadecimal numbers, each separated by a colon. Example: fe80:11a1:ac15:e9gf:fe884:edb0:ddee:fea3.

Many network devices are now provisioned with both an IPv4 and an IPv6 address. The DNS name server can resolve domain names to both IPv4 and IPv6 addresses.

DNS settings for your domain

Whether the DNS server for your domain is hosted by a third party or managed in-house, you'll need to configure it for each host type you're using. Host types include web, email, or other services you're using.

As the administrator for your company, you want to set up a DNS server by using Azure DNS. In this instance, the DNS server will act as a start of authority (SOA) for your domain.

DNS record types

Configuration information for your DNS server is stored as a file within a zone on your DNS server. Each file is called a record. The following record types are the most commonly created and used:

- A is the host record, and is the most common type of DNS record. It maps the domain or host name to the IP address.
- CNAME is a Canonical Name record that's used to create an alias from one domain name to another domain name. If you had different domain names that all accessed the same website, you would use CNAME.
- MX is the mail exchange record. It maps mail requests to your mail server, whether hosted on-premises or in the cloud.
- TXT is the text record. It's used to associate text strings with a domain name. Azure and Microsoft 365 use TXT records to verify domain ownership.

Additionally, there are the following record types:

- Wildcards
- CAA (certificate authority)
- NS (name server)
- SOA (start of authority)
- SPF (sender policy framework)
- SRV (server locations)

The SOA and NS records are created automatically when you create a DNS zone by using Azure DNS.

Record sets

Some record types support the concept of record sets, or resource record sets. A record set allows for multiple resources to be defined in a single record. For example, here is an A record that has one domain with two IP addresses:

						Copy
www.wideworldimports.com.	3600	IN	A	127.0.0.1		
www.wideworldimports.com.	3600	IN	A	127.0.0.2		

SOA and CNAME records can't contain record sets.

What is Azure DNS?

Azure DNS allows you to host and manage your domains by using a globally distributed name server infrastructure. It allows you to manage all of your domains by using your existing Azure credentials.

Azure DNS acts as the SOA for the domain.

You can't use Azure DNS to register a domain name. You use a third-party domain registrar to register your domain.

Why use Azure DNS to host your domain?

Azure DNS is built on the Azure Resource Manager service, which offers the following benefits:

- Improved security
- Ease of use
- Private DNS domains
- Alias record sets

At this time, Azure DNS doesn't support Domain Name System Security Extensions. If you require this security extension, you should host those portions of your domain with a third-party provider.

Security features

Azure DNS provides the following security features:

- Role-based access control, which gives you fine-grained control over users' access to Azure resources. You can monitor their usage and control the resources and services to which they have access.
- Activity logs, which let you track changes to a resource and pinpoint where faults occurred.
- Resource locking, which gives a greater level of control to restrict or remove access to resource groups, subscriptions, or any Azure resources.

Ease of use

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

You can manage your domains and records by using the Azure portal, Azure PowerShell cmdlets, or the Azure CLI. Applications that require automated DNS management can integrate with the service by using the REST API and SDKs.

Private domains

Azure DNS handles the translation of external domain names to an IP address. Azure DNS lets you create private zones. These provide name resolution for virtual machines (VMs) within a virtual network, and between virtual networks, without having to create a custom DNS solution. This allows you to use your own custom domain names rather than the Azure-provided names.

To publish a private DNS zone to your virtual network, you'll specify the list of virtual networks that are allowed to resolve records within the zone.

Private DNS zones have the following benefits:

- There's no need to invest in a DNS solution. DNS zones are supported as part of the Azure infrastructure.
- All DNS record types are supported: A, CNAME, TXT, MX, SOA, AAAA, PTR, and SRV.
- Host names for VMs in your virtual network are automatically maintained.
- Split-horizon DNS support allows the same domain name to exist in both private and public zones. It resolves to the correct one based on the originating request location.

Alias record sets

Alias records sets can point to an Azure resource. For example, you can set up an alias record to direct traffic to an Azure public IP address, an Azure Traffic Manager profile, or an Azure Content Delivery Network endpoint.

The alias record set is supported in the following DNS record types:

- A
- AAAA
- CNAME

Check your knowledge

1. What does Azure DNS allow you to do? *

- Manage the security and access to your website.
- Register new domain names, removing the need to use a domain registrar.
X Azure DNS isn't a domain registrar. It hosts your domain, and allows you to manage DNS zone records.
- Manage and host your registered domain and associated records.
- Azure DNS allows you to host your registered domains. You can control and configure the domain records, like A, CNAME, MX, and setup alias records.

2. What security features does Azure DNS provide? *

- Role-based access control, activity logs, and resource locking.
✓ Azure DNS is built on Azure Resource Manager, which provides security across all resources in Azure DNS.
- Role-based access control, activity logs, and Azure threat detection
- Role-based access control, activity logs, and Azure infrastructure security

3. What type of DNS record should you create to map one or more IP addresses against a single domain? *

- CNAME
X The CNAME record maps a domain name to another domain name.
- A or AAAA
✓ The A or AAAA record maps an IP address to a domain. Multiple IP addresses are known as a record set.
- SOA

Using Azure Firewall

Azure Firewall

- Filter traffic with a Platform as a Service (PaaS) firewall
- Fully qualified domain name (FQDN) support

The diagram illustrates the architecture of Azure Firewall. It shows a VNet with two subnets: 'AzureFirewallSubnet' and 'Default'. A red firewall appliance is placed in the 'AzureFirewallSubnet'. Traffic flows from the internet (represented by a globe icon) through the firewall to a computer icon, and vice versa. The VNet boundary is indicated by a dashed line.

Para poder implementarlo es necesario crear una subnet con slash mínimo de 26 llamada AzureFirewallSubnet dentro de nuestra vnet donde quereos poner el firewall

Azure Firewall Features

The diagram shows five features of Azure Firewall, each represented by an orange circle connected to a central hub labeled 'Azure Firewall Features':

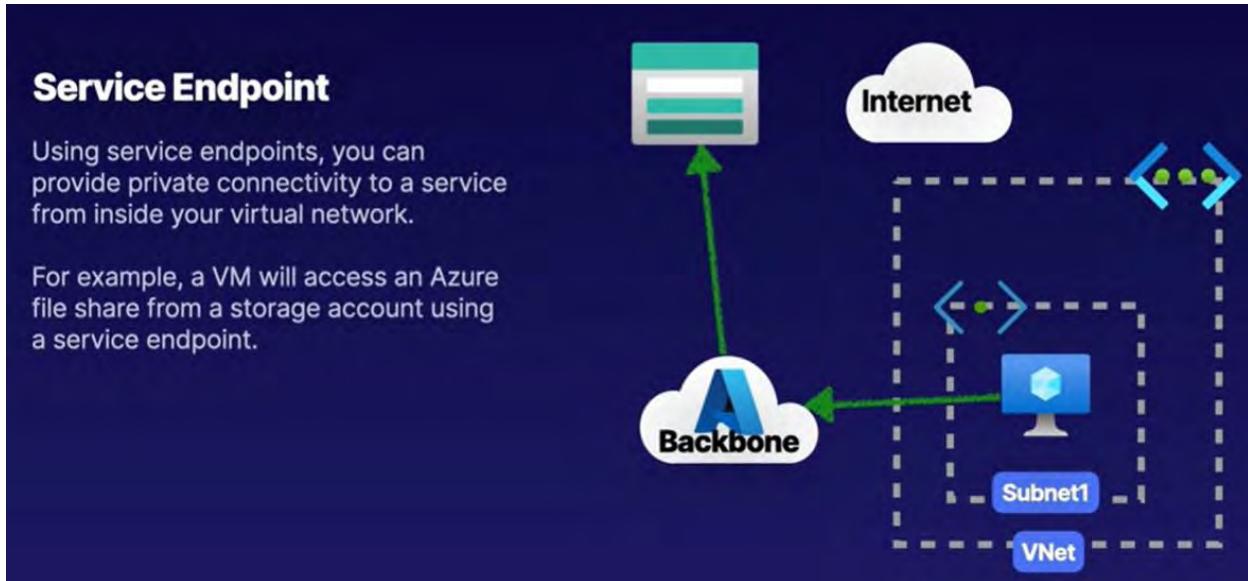
- DNAT and SNAT**: Configure outbound/inbound NAT rules for your networks.
- Network Rules**: Configure network (Layer 4) rules for what traffic is allowed.
- App Rules**: Configure rules for filter websites visited from your network.
- Threat Intel**: Identify malicious IPs and domains.
- Monitoring**: Integrate with Azure Monitor to capture firewall traffic.

Se tiene que crear un route table que envie el trafico de la subnet que queramos a la subnet con el azure firewall

Las reglas las añadimos en el azure firewall y todo lo de la subnet que quieras pasara por estas reglas

Using Service Endpoints

Sirven para conectarte a PAAS atraves del backbone de azure y no viajar atraves de internet



Service Endpoint

- Enabled *per subnet*
- **Not** all services are supported
- Supported services *differ per region*
- Does **not** give services a private IP
- Provides source IP as private IP
- Firewalls can enhance security (*optional*)

El Service endpoint es configurado por subnet

Puedes crear políticas en endpoints policies para que la subnet solo tenga acceso en especifico a una storage account o suscripción

The screenshot shows the Azure portal interface for creating a service endpoint policy. On the left, there's a navigation bar with 'Basics', 'Policy definitions' (which is selected), 'Tags', and 'Review + create'. Below this, sections for 'Resources' (+ Add a resource), 'Service' (Microsoft.Storage), 'Allowed Resources', and 'Resource Group' (Resource Group: P2-Real Hands-On Labs, Resource: cloudemochashell) are visible. A large play button icon is centered. On the right, a modal window titled 'Add a resource' is open, showing fields for 'Service' (Microsoft.Storage), 'Scope' (Single account), 'Subscription' (P2-Real Hands-On Labs), 'Resource group' (1-494ae2c6-playground-sandbox), and 'Resource' (cloudemochashell).

Using Private Endpoints

Es básicamente como Service endpoint pero aquí le asignamos una Ip privado a alguno de nuestros servicios y por medio de esa ip accederemos a ellos

The diagram illustrates Azure Private Endpoint connectivity. It shows a cloud icon labeled 'A' containing an 'Azure Files' icon. This is connected via a dashed line to a 'Subnet1' icon within a 'VNet' boundary. A double-headed arrow indicates the bidirectional connectivity between the cloud service and the subnet.

Private Endpoint

Using Azure Private Link, you can connect your services as **connected resources** in your network with a private IP known as a private endpoint.

Private endpoint connectivity for:

- Azure services
- Customer/partner services

Provides direct service (sub-resource) mapping.

Para crear un private endpoint nos vamos a Private link center

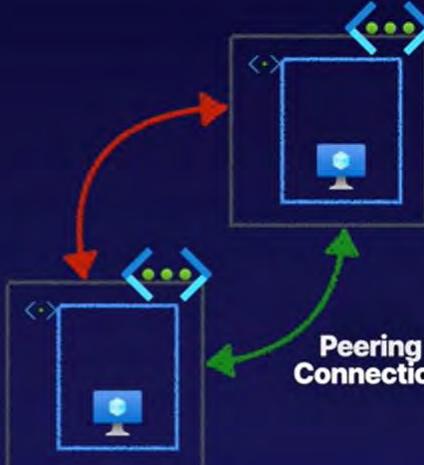
Configuring Azure Vnet Peering

Describing VNet Peering

Network Connectivity

Default Connectivity
While intra-network traffic and outbound internet traffic is allowed, virtual networks are by default isolated.

VNet Peering
Bridge together virtual networks to allow connectivity between these networks.



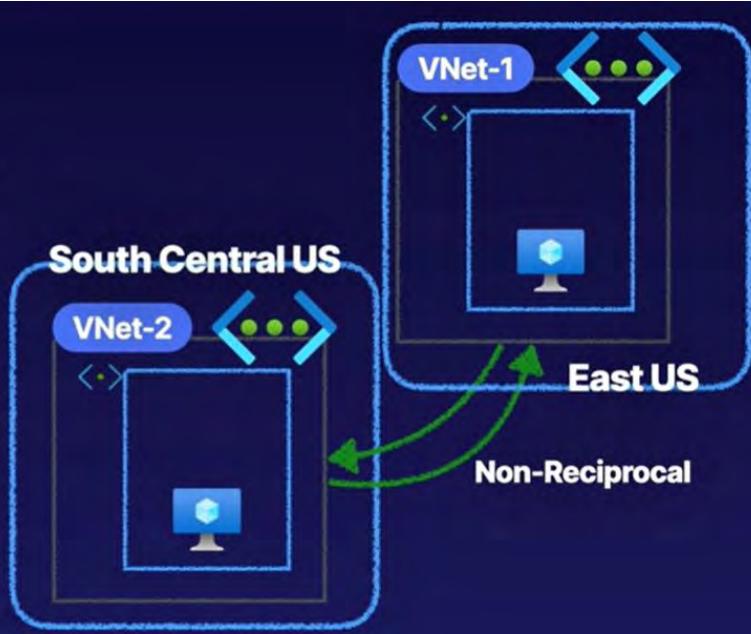
La conexión se debe configurar en ambos sentidos

Non-Reciprocal

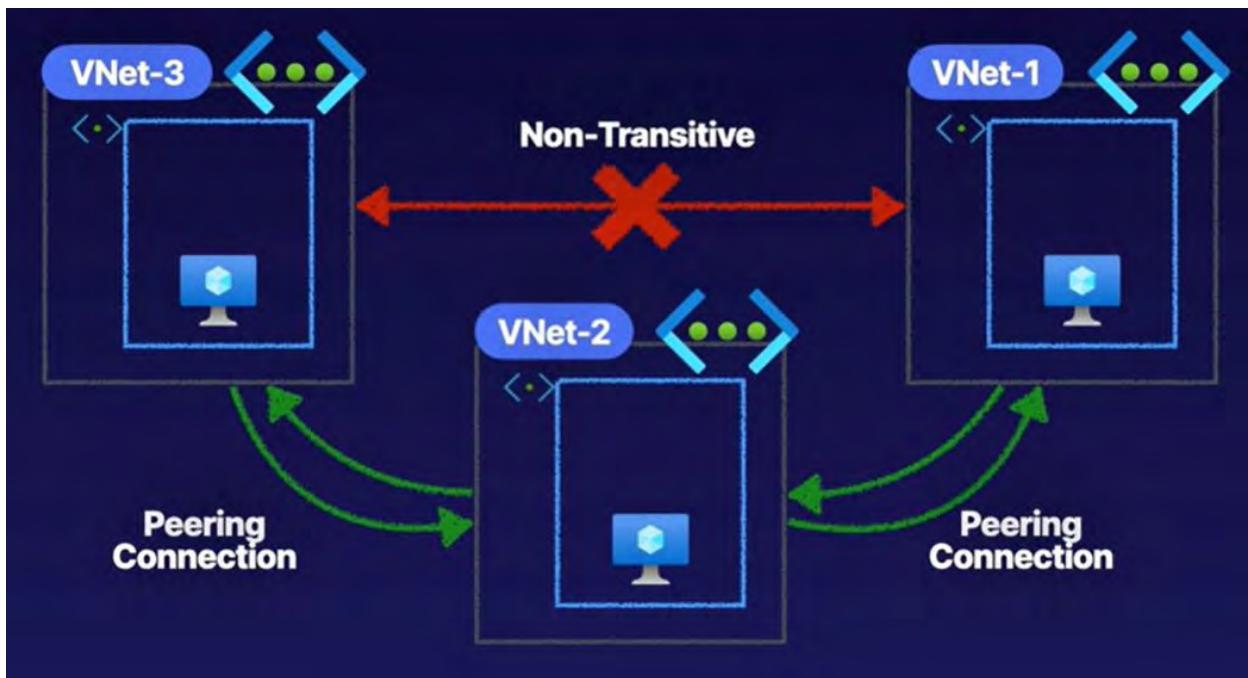
Connection must be established in both directions

Global Connectivity

Peerings can be same region or cross-region (global)



El vnet peering no es transitivo



El tráfico de las vnet peering es a través del backbone de azure

Benefits of VNet Peering

Benefits

- Low-latency, high-bandwidth connections
- Cross-network communications
- Data transfer between/across:
 - Subscriptions
 - AAD tenants via Azure roles
 - Azure regions

The slide is titled "Benefits of VNet Peering". It features a bulleted list of benefits: low-latency, high-bandwidth connections; cross-network communications; and data transfer between/across subscriptions, AAD tenants via Azure roles, and Azure regions. To the right of the list is a diagram showing two virtual network boxes (VNet-1 and VNet-2) connected by a green curved arrow, representing a peering connection. A large play button icon is overlaid on the diagram.

El rango de IPs o CIDR tiene que ser diferente para poder hacer el peering ejemplo 172.0.0.1/16 y 192-168.1.0 puedes hacer el peering

Es las settings de la vnet ponemos el peering

Diagnose and solve problems

Settings

Address space

Connected devices

Subnets

DDoS protection

Firewall

Security

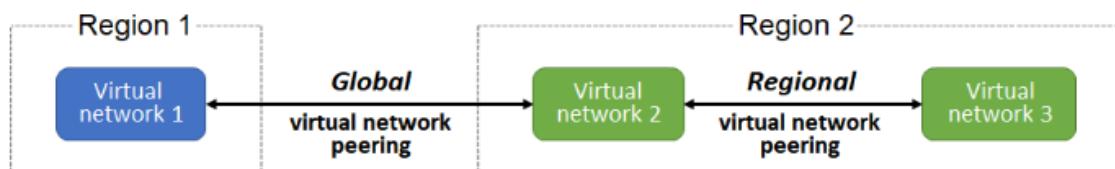
DNS servers

Peerings

Things to know about Azure Virtual Network peering

Let's examine some prominent characteristics of Azure Virtual Network peering.

- There are two types of Azure Virtual Network peering: *regional* and *global*.



- Regional virtual network peering connects Azure virtual networks that exist in the same region.
- Global virtual network peering connects Azure virtual networks that exist in different regions.
- You can create a regional peering of virtual networks in the same Azure public cloud region, or in the same China cloud region, or in the same Microsoft Azure Government cloud region.
- You can create a global peering of virtual networks in any Azure public cloud region, or in any China cloud region.
- Global peering of virtual networks in different Azure Government cloud regions isn't permitted.
- After you create a peering between virtual networks, the individual virtual networks are still managed as separate resources.

Things to consider when using Azure Virtual Network peering

Consider the following benefits of using Azure Virtual Network peering.

Benefit	Description
Private network connections	When you implement Azure Virtual Network peering, network traffic between peered virtual networks is private. Traffic between the virtual networks is kept on the Microsoft Azure backbone network. No public internet, gateways, or encryption is required in the communication between the virtual networks.
Strong performance	Because Azure Virtual Network peering utilizes the Azure infrastructure, you gain a low-latency, high-bandwidth connection between resources in different virtual networks.
Simplified communication	Azure Virtual Network peering lets resources in one virtual network communicate with resources in a different virtual network, after the virtual networks are peered.
Seamless data transfer	You can create an Azure Virtual Network peering configuration to transfer data across Azure subscriptions, deployment models, and across Azure regions.
No resource disruptions	Azure Virtual Network peering doesn't require downtime for resources in either virtual network when creating the peering, or after the peering is created.

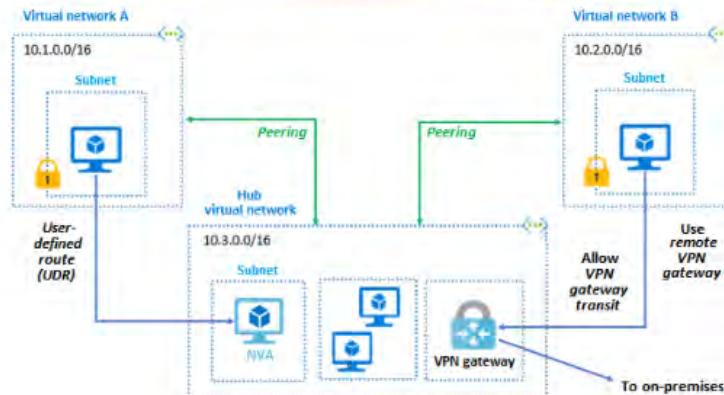
Determine gateway transit and connectivity

100 XP

2 minutes

When virtual networks are peered, you can configure Azure VPN Gateway in the peered virtual network as a transit point. In this scenario, a peered virtual network uses the remote VPN gateway to gain access to other resources.

Consider a scenario where three virtual networks in the same region are connected by virtual network peering. Virtual network A and virtual network B are each peered with a hub virtual network. The hub virtual network contains several resources, including a gateway subnet and an Azure VPN gateway. The VPN gateway is configured to allow VPN gateway transit. Virtual network B accesses resources in the hub, including the gateway subnet, by using a remote VPN gateway.



Things to know about Azure VPN Gateway

Let's take a closer look at how Azure VPN Gateway is implemented with Azure Virtual Network peering.

- A virtual network can have only one VPN gateway.
- Gateway transit is supported for both regional and global virtual network peering.
- When you allow VPN gateway transit, the virtual network can communicate to resources outside the peering. In our sample illustration, the gateway subnet gateway within the hub virtual network can complete tasks such as:
 - Use a site-to-site VPN to connect to an on-premises network.
 - Use a vnet-to-vnet connection to another virtual network.
 - Use a point-to-site VPN to connect to a client.
- Gateway transit allows peered virtual networks to share the gateway and get access to resources. With this implementation, you don't need to deploy a VPN gateway in the peer virtual network.
- You can apply network security groups in a virtual network to block or allow access to other virtual networks or subnets. When you configure virtual network peering, you can choose to open or close the network security group rules between the virtual networks.

Things to know about creating virtual network peering

There are a few points to review before we look at how to create the peering in the Azure portal.

- To implement virtual network peering, your Azure account must be assigned to the [Network Contributor](#) or [Classic Network Contributor](#) role. Alternatively, your Azure account can be assigned to a custom role that can complete the necessary peering actions. For details, see [Permissions](#).
- To create a peering, you need two virtual networks.
- The second virtual network in the peering is referred to as the *remote network*.
- Initially, the virtual machines in your virtual networks can't communicate with each other. After the peering is established, the machines can communicate within the peered network based on your configuration settings.

How to check your peering status

In the Azure portal, you can check the connectivity status of the virtual networks in your virtual network peering. The status conditions depend on how your virtual networks are deployed.

ⓘ Important

Your peering isn't successfully established until both virtual networks in the peering have a status of **Connected**.

- For deployment with the Azure Resource Manager, the two primary status conditions are **Initiated** and **Connected**. For the classic deployment model, the **Updating** status condition is also used.
- When you create the initial peering *to* the second (remote) virtual network from the first virtual network, the peering status for the first virtual network is **Initiated**.
- When you create the subsequent peering *from* the second virtual network to the first virtual network, the peering status for both the first and remote virtual networks is **Connected**. In the Azure portal, you can see the status for the first virtual network change from **Initiated** to **Connected**.

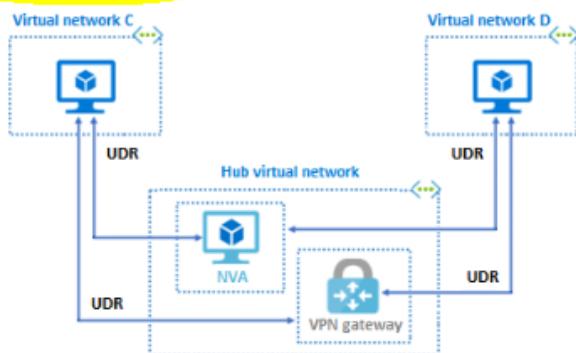
Things to know about extending peering

There are a few ways to extend the capabilities of your peering for resources and virtual networks outside your peering network:

- Hub and spoke networks
- User-defined routes
- Service chaining

You can implement these mechanisms and create a multi-level hub and spoke architecture. These options can help overcome the limit on the number of virtual network peerings per virtual network.

The following diagram shows a hub and spoke virtual network with an NVA and VPN gateway. The hub and spoke network is accessible to other virtual networks via user-defined routes and service chaining.



Mechanism	Description
Hub and spoke network	When you deploy a hub-and-spoke network, the hub virtual network can host infrastructure components like a network virtual appliance (NVA) or Azure VPN gateway. All the spoke virtual networks can then peer with the hub virtual network. Traffic can flow through NVAs or VPN gateways in the hub virtual network.
User-defined route (UDR)	Virtual network peering enables the next hop in a user-defined route to be the IP address of a virtual machine in the peered virtual network, or a VPN gateway.
Service chaining	Service chaining lets you define UDRs. These routes direct traffic from one virtual network to an NVA or VPN gateway.

1. When virtual networks are successfully peered, what's the peering status for both virtual networks in the peering? *

Initiated

Connected

✓ Correct. The peering isn't successfully established until the peering status for both virtual networks is Connected.

Peered

2. What approach enables peered virtual networks to share the gateway and get access to resources? *

Point-to-site connectivity

Transitivity

Gateway transit

✓ Correct. Gateway transit allows peered virtual networks to share the gateway and get access to resources.

3. How is Azure Virtual Network peering best described? *

Traffic between virtual networks is kept on the Microsoft backbone network.

✓ Correct. The Azure backbone handles traffic between virtual networks in a virtual network peering.

Virtual network peering disrupts other resources.

Peered virtual networks must be in the same region.

1. Why would you use a custom route in a virtual network? *

- To load balance the traffic within your virtual network.
 - To connect to your Azure virtual machines using RDP or SSH.
 - To control the flow of traffic within your Azure virtual network.
- ✓ This is the correct answer. Custom routes are used to override the default Azure routing so that you can route traffic through a network virtual appliance (NVA).
- To connect to resources in another virtual network hosted in Azure.

2. Why might you use virtual network peering? *

- To connect virtual networks together in the same region or across regions.
- ✓ This is the correct answer. Virtual network peering is used to connect multiple virtual networks together. Once peered, the networks become one network, and resources across virtual networks can communicate with one another.
- To assign public IP addresses to all of your resources across multiple virtual networks.
 - So that load balancers can control traffic flow across your virtual networks.
 - To run custom reports that scan and identify what resources are running across all of your virtual networks, as opposed to running reports on each virtual network.

Implementing VPNs

Es como el vnet peering pero nos permite conectar también redes on-prem y estas conexiones se hacen 'por internet'

El tráfico tiene un Ipsec tunnel que encripta la info

VPN Gateway vs. VNet Peering

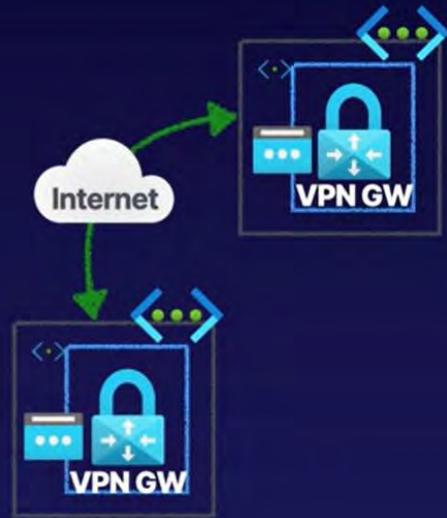
A CLOUD G

VPN Gateway

Establishes connectivity between VNets, similar to VNet peering.

Components:

- VNet gateway for VPN gateway
- Gateway subnet
- Public IP per VNet gateway
- IPsec tunnel for encryption



El VPN Gateway tiene transitive traffic

Routing Types

Policy-Based

- Static routing via policy declarations
- Legacy on-premises VPN devices
- Only supports IKEv1
- Only Basic SKU

Route-Based

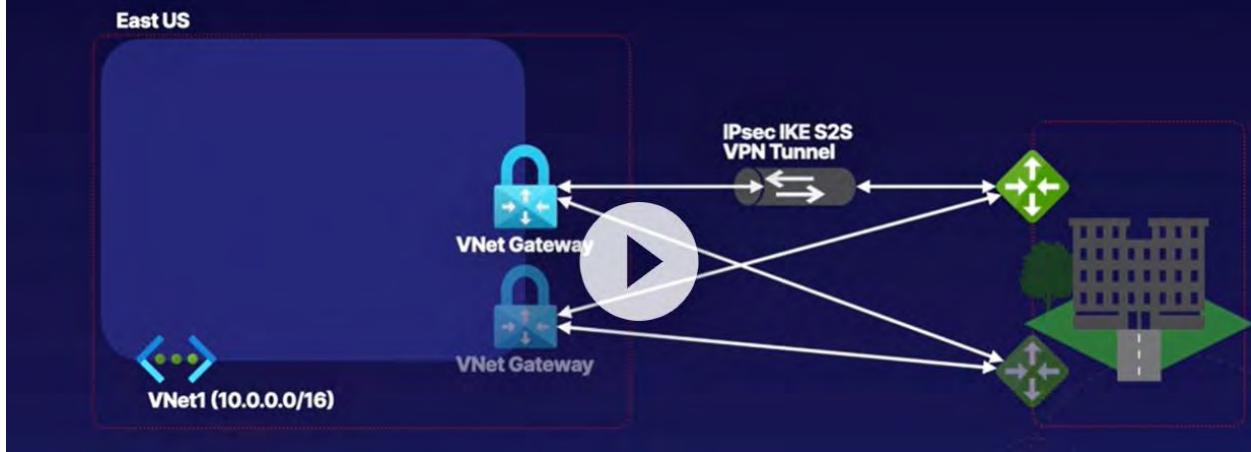
- Static and dynamic routing
- Resilient to topology changes
- Can coexist with ExpressRoute

VPN Gateway SKUs

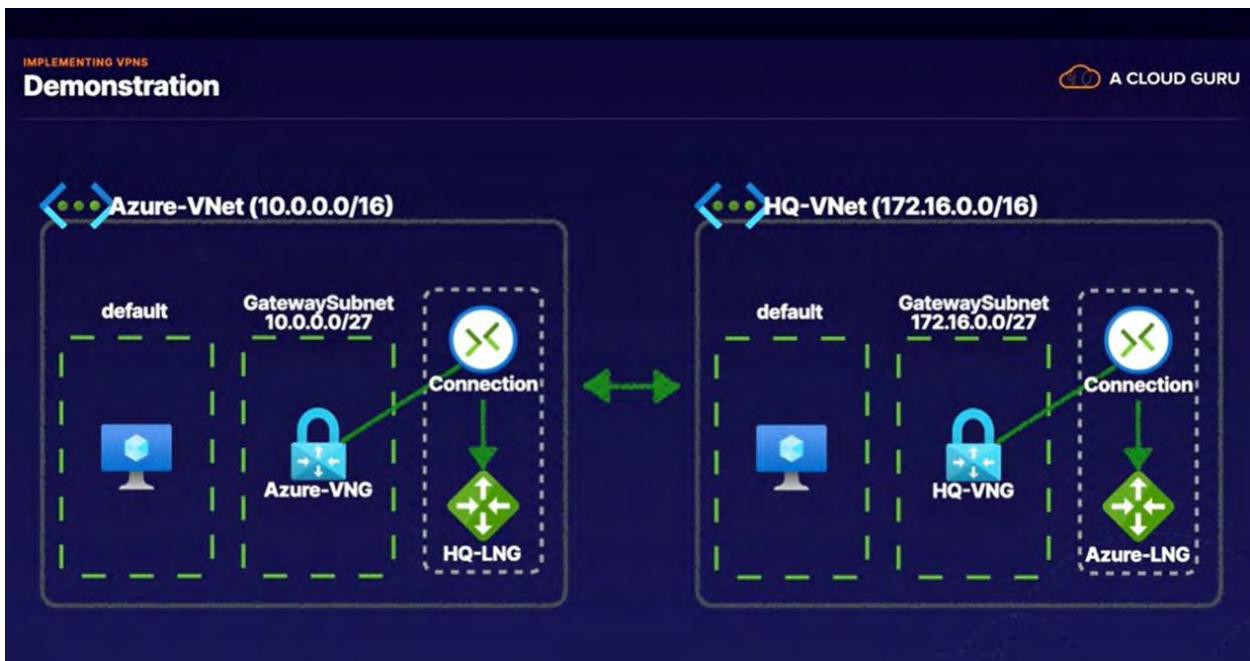
SKU	Site-to-Site Tunnels	Throughput	BGP Support
Basic	Max: 10	100 Mbps	Not supported
VpnGw1AZ	Max: 30	650 Mbps	Supported
VpnGw2AZ	Max: 30	1 Gbps	Supported
VpnGw3AZ	Max: 30	1.25 Gbps	Supported

Basic solo se debería usar en dev/test workloads y no puedes migrar de skus, tienes que volver a implementar el Gateway

Puedes tener 2 vnet Gateway activadas (active-active) o 1 y una(active passive), para si una falla entre la otra y tome el tráfico

Active-Active vs. Active-Passive

La Gateway subnet debe ser de 27 de slash



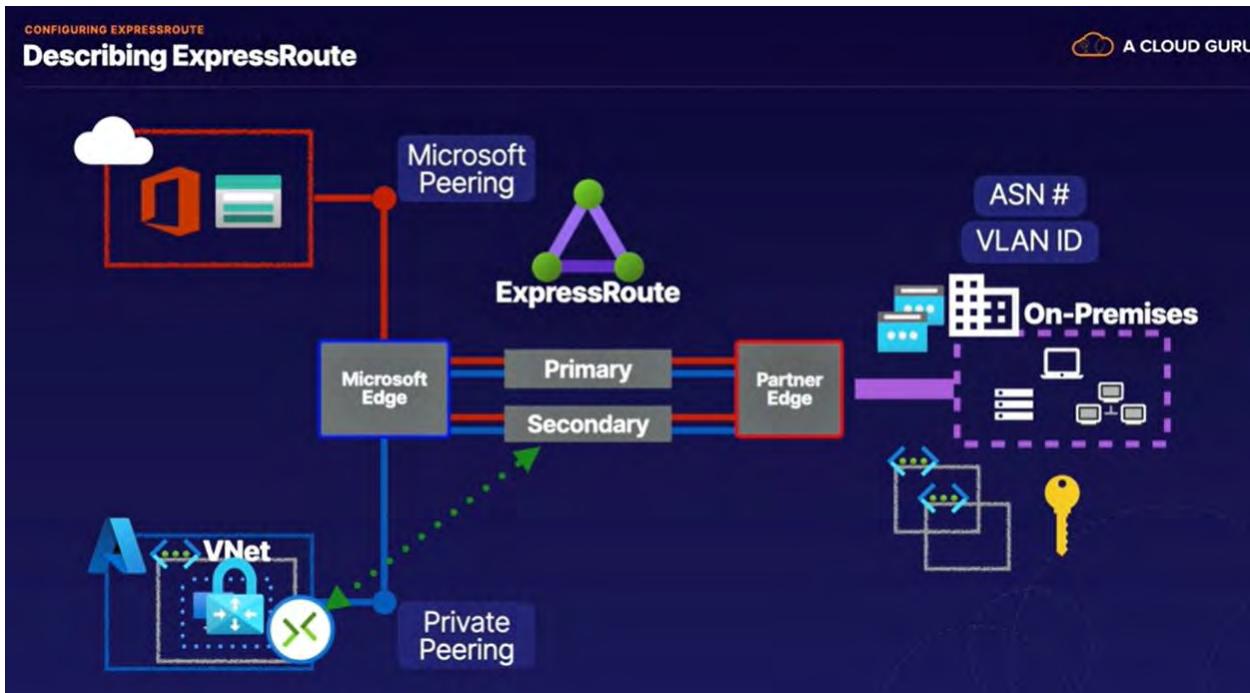
PASOS:

- 1.- Crear vnet Gateway
- 2.- Crear Gateway subnet addred range
- 3.- crear los local network gateways
- 4.- local network gateway en setting y connect se conectan las 2 local networks



- VNet-to-VNet
- Site-to-Site
- Point-to-Site
- IPsec tunnel for encryption

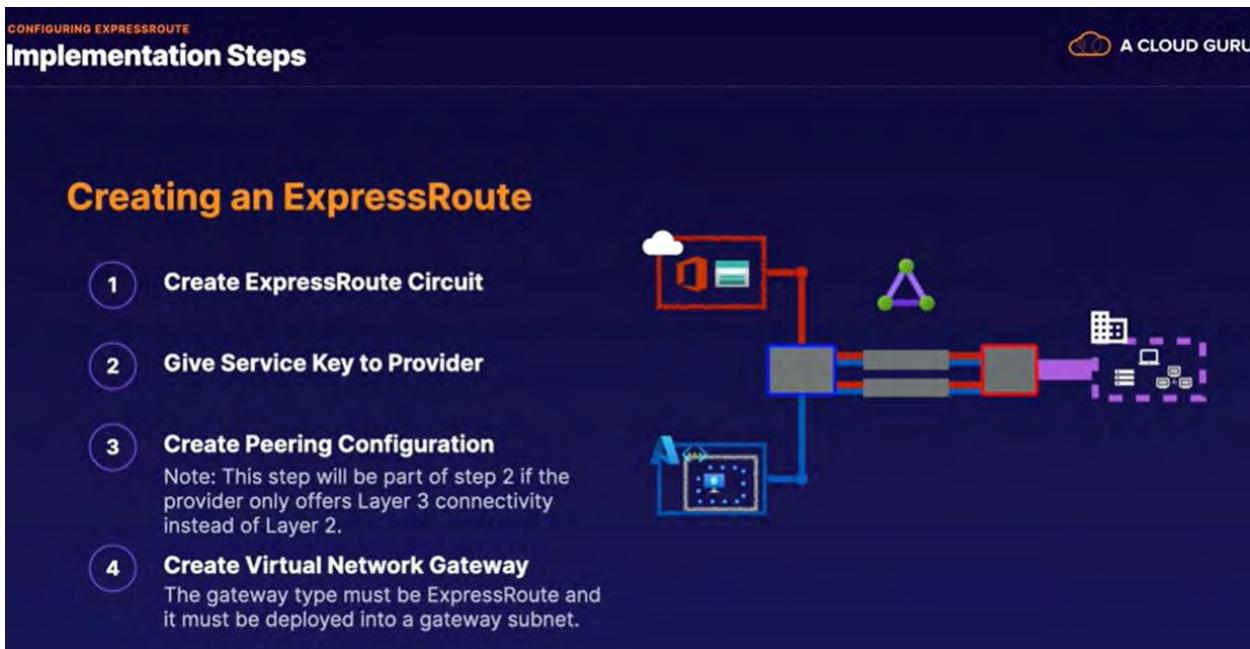
Configuring ExpressRoute



Es para hacer conexiones físicas dedicadas, esta conexión no está cifrada por default.

En on prem se necesitan 4 redes con slash 30 para configurar express route, shared key, ASN VLAN ID

En Azure necesita una vnet con su subnet Gateway y vpn Gateway



Create ExpressRoute

Basics Configuration Tags Review + create

Select Provider if you are connecting to a service provider in order to access Microsoft's network. Select Direct if you have an ExpressRoute Direct resource and want to use it to connect directly into Microsoft's global network.

Port type *

Provider

Direct

Create new or import from classic *

Create new

Import

Provider *

SKU *

Local

Standard

Premium

Billing model *

Metered

Unlimited

El provider puede ser Microsoft u otro que elijamos

Podemos elegir de 50 Mbps a 10 Gbps la conexión

SKU:

- Local nos da conexión de azure con el on-prem a 1 o 2 regiones de azure
- Standard:nos da acceso a la conexión a todas las regiones de azure
- - Premium: nos da global connectivity

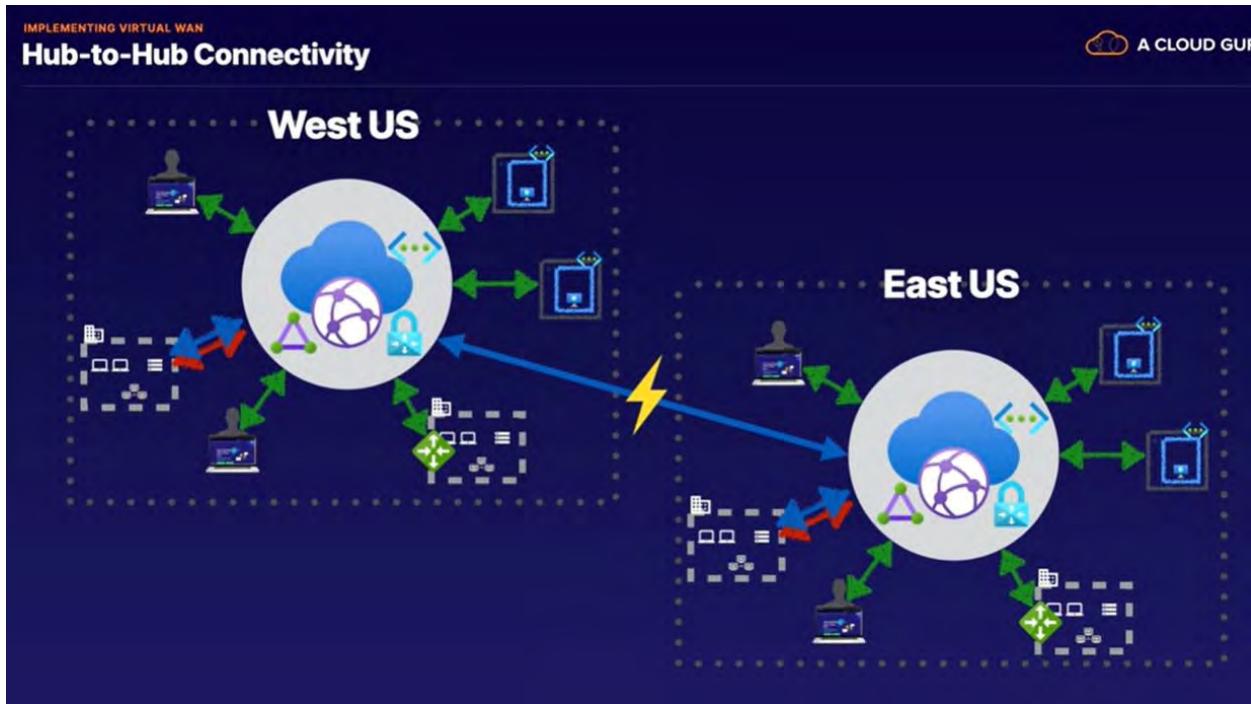
Billing: todo lo que salga de on-prem a azure es gratis, por lo que se paga es por el trafico de Microsoft hacia on-prem atraves el express route. Podemos elegir pagar por uso o ilimitado



Bgp: border Gateway protocol

Implementing Virtual WAN

Es como una manera o servicio de manejar todas tus conexiones de red en una plataforma.



En este ejemplo conectando 2 wan conectaríamos todas las redes dentro de ellas



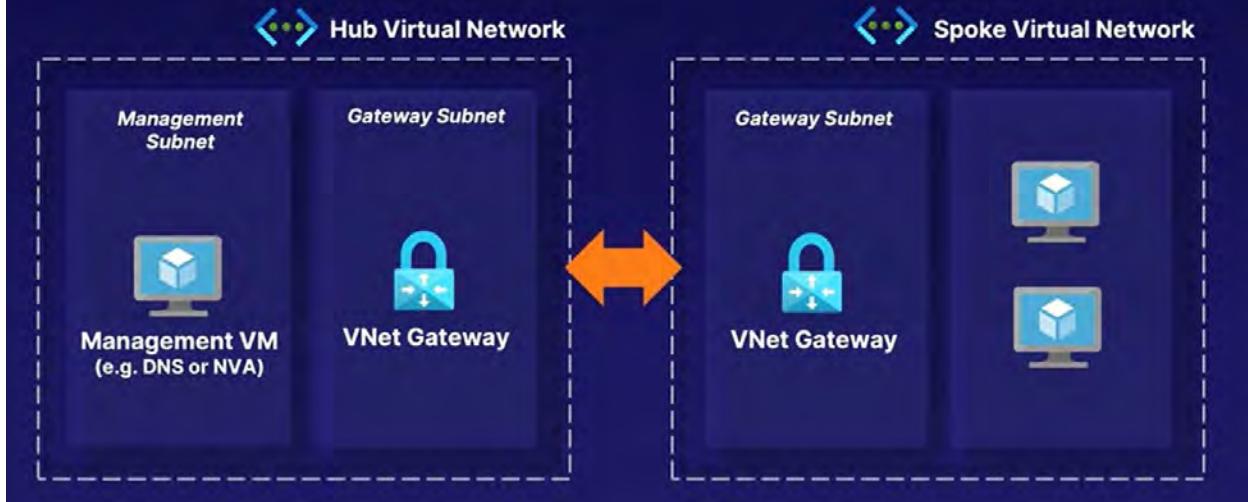
Podemos tener un HUB por región

Las conexiones van dentro de cada virtual HUB

Puedes asegurar tu wan con azure firewall y firewall manager

Hub-Spoke

A CLOUD GURU



Review system routes

✓ 100 XP

2 minutes

Azure uses *system routes* to direct network traffic between virtual machines, on-premises networks, and the internet. Information about the system routes is recorded in a *route table*.

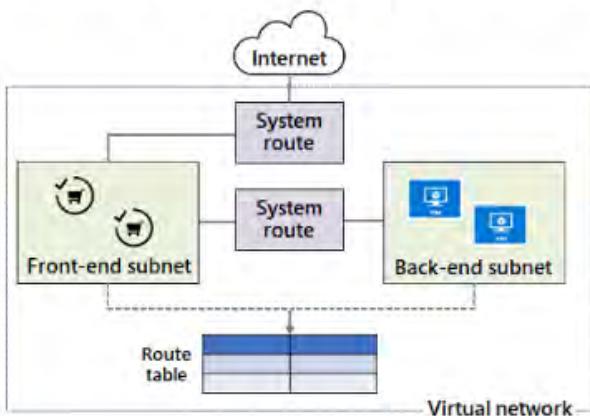
Things to know about system routes

Let's take a closer look at how Azure implements system routes.

- Azure uses system routes to control traffic for virtual machines in several scenarios:
 - Traffic between virtual machines in the same subnet
 - Traffic between virtual machines in different subnets in the same virtual network
 - Traffic from virtual machines to the internet
- A route table contains a set of rules (called *routes*) that specifies how packets should be routed in a virtual network.
- Route tables record information about the system routes, where the tables are associated to subnets.
- Each packet leaving a subnet is handled based on the associated route table.
- Packets are matched to routes by using the destination. The destination can be an IP address, a virtual network gateway, a virtual appliance, or the internet.
- When a matching route can't be found, the packet is dropped.

Business scenario

Suppose you have a virtual network with two subnets. In this configuration, you can use Azure system routes to control communication between the subnets and between subnets and the internet. A front-end subnet can use a system route to access the internet. A back-end subnet can use a system route to access the front-end subnet. Both subnets access a route table. The following illustration highlights this scenario:



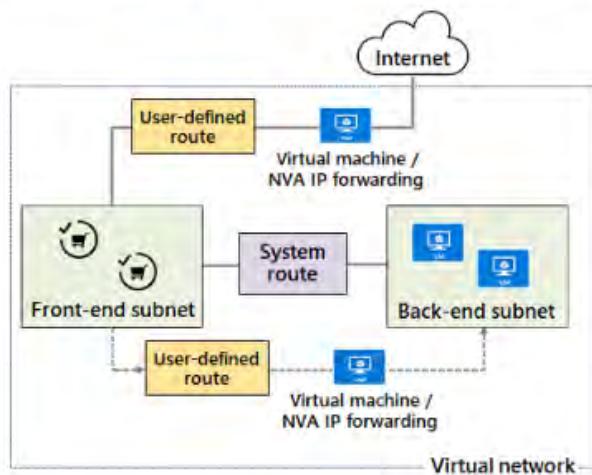
Things to know about user-defined routes

Let's examine the characteristics of user-defined routes.

- UDRs control network traffic by defining routes that specify the *next hop* of the traffic flow.
- The next hop can be one of the following targets:
 - Virtual network gateway
 - Virtual network
 - Internet
 - Network virtual appliance (NVA)
- Similar to system routes, UDRs also access route tables.
- Each route table can be associated to multiple subnets.
- Each subnet can be associated to one route table only.
- There are no charges for creating route tables in Microsoft Azure.

Business scenario

Suppose you have a virtual machine that performs a network function like routing, firewalling, or WAN optimization. You want to direct certain subnet traffic to the NVA. To accomplish this configuration, you can place an NVA between subnets or between one subnet and the internet. The subnet can use a UDR to access the NVA and then the internet. The subnet can use another UDR and NVA to access the back-end subnet. The following illustration highlights this scenario:



Determine service endpoint uses

✓ 100 XP

3 minutes

A virtual network service endpoint provides the identity of your virtual network to the Azure service. After service endpoints are enabled in your virtual network, you can secure Azure service resources to your virtual network by adding a virtual network rule to the resources.

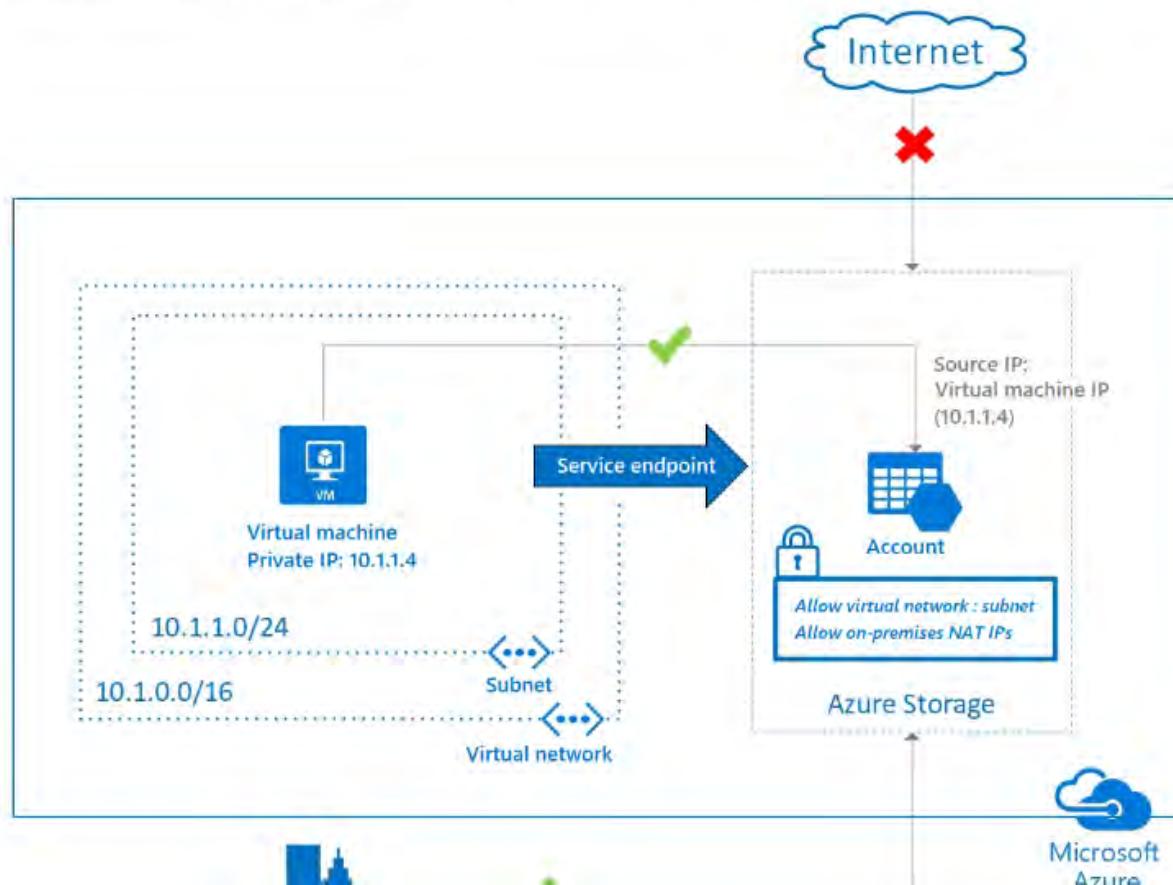
Today, Azure service traffic from a virtual network uses public IP addresses as source IP addresses. With service endpoints, service traffic switches to use virtual network private addresses as the source IP addresses when accessing the Azure service from a virtual network. This switch allows you to access the services without the need for reserved public IP addresses that are typically used in IP firewalls.

Things to know about service endpoints

Review the following characteristics of service endpoints.

- Service endpoints can extend your virtual network identity to your Azure services to secure your service resources.
- You secure your Azure service resources to your virtual network by using virtual network rules.
- Virtual network rules can remove public internet access to resources, and allow traffic only from your virtual network.
- Service endpoints always take service traffic directly from your virtual network to the service on the Microsoft Azure backbone network.
- Service endpoints are configured through the subnet. No extra overhead is required to maintain the endpoints.

The following illustration shows a virtual machine connecting to the Azure service through a service endpoint. A virtual machine in a subnet accesses an Azure Storage account through a service endpoint. Virtual network rules allow the virtual machine to access the Azure service resource, but not communicate with the internet.



Things to consider when using service endpoints

There are several scenarios where using service endpoints can be advantageous. Review the following points and think about how you can implement service endpoints in your configuration.

- Consider improved security for resources. Implement service endpoints to improve the security of your Azure service resources. When service endpoints are enabled in your virtual network, you secure Azure service resources to your virtual network with virtual network rules. The rule improves security by fully removing public internet access to resources, and allowing traffic only from your virtual network.
- Consider optimal routing for service traffic. Routes in your virtual network that force internet traffic to your on-premises or network virtual appliances also typically force Azure service traffic to take the same route as the internet traffic. This traffic control process is known as *forced-tunneling*. Service endpoints provide optimal routing for Azure service traffic to allow you to circumvent forced tunneling.
- Consider direct traffic to the Microsoft network. Use service endpoints to keep traffic on the Azure backbone network. This approach allows you to continue auditing and monitoring outbound internet traffic from your virtual networks, through forced-tunneling, without impacting service traffic. Learn more about user-defined routes and forced-tunneling.
- Consider easy configuration and maintenance. Configure service endpoints in your subnets for simple setup and low maintenance. You no longer need reserved public IP addresses in your virtual networks to secure Azure resources through an IP firewall. There are no NAT or gateway devices required to set up the service endpoints.

Note

With service endpoints, the virtual machine IP addresses switch from public to private IPv4 addresses. Existing Azure service firewall rules that use Azure public IP addresses stop working after the switch. Ensure Azure service firewall rules allow for this switch before you set up service endpoints. You might also experience temporary interruption to service traffic from this subnet while configuring service endpoints.

Service	Availability	Description
Azure Storage	Generally available in all Azure regions	This endpoint gives traffic an optimal route to the Azure Storage service. Each Storage account supports up to 100 virtual network rules.
Azure SQL Database and Azure SQL Data Warehouse	Generally available in all Azure regions	A firewall security feature controls whether your database accepts communication from particular subnets in virtual networks. This feature applies to the database server for your single databases and elastic pool in SQL Database or your databases in SQL Data Warehouse.
Azure Database for PostgreSQL and Azure Database for MySQL	Generally available in Azure regions where database service is available	Virtual network service endpoints and rules extend the private address space of a virtual network to your Azure Database for PostgreSQL server and Azure Database for MySQL server.
Azure Cosmos DB	Generally available in all Azure regions	You can configure the Azure Cosmos DB account to allow access only from a specific subnet of virtual network. Enable service endpoints to access Azure Cosmos DB on the subnet within a virtual network. Traffic from the subnet is sent to Azure Cosmos DB with the identity of the subnet and virtual network. After the Azure Cosmos DB service endpoint is enabled, you can limit access to the subnet by adding it to your Azure Cosmos DB account.
Azure Key Vault	Generally available in all Azure regions	The virtual network service endpoints for Key Vault allow you to restrict access to a specified virtual network. The endpoints also allow you to restrict access to a list of IPv4 (internet protocol version 4) address ranges. Any user connecting to your key vault from outside those sources is denied access.
Azure Service Bus and Azure Event Hubs	Generally available in all Azure regions	The integration of Service Bus with virtual network service endpoints enables secure access to messaging capabilities from workloads like virtual machines that are bound to virtual networks. The network traffic path is secured on both ends.

Identify private link uses

100 XP

2 minutes

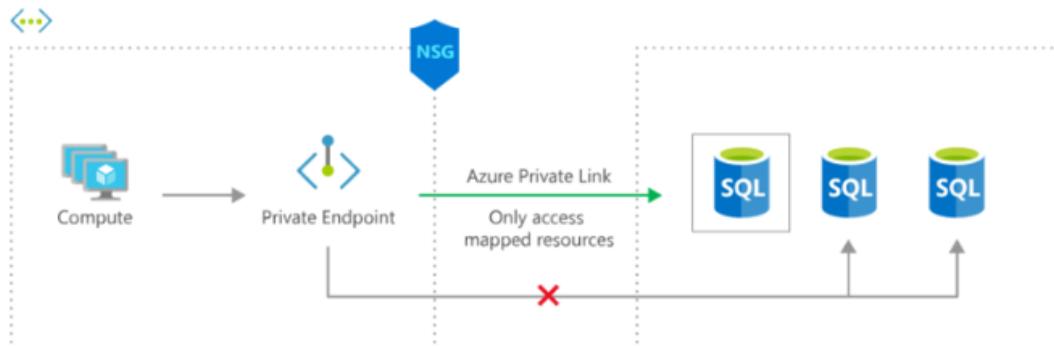
Azure Private Link provides private connectivity from a virtual network to Azure platform as a service (PaaS), customer-owned, or Microsoft partner services. It simplifies the network architecture and secures the connection between endpoints in Azure by eliminating data exposure to the public internet.

Things to know about Azure Private Link

Let's examine the characteristics of Azure Private Link and network routing configurations.

- Azure Private Link keeps all traffic on the Microsoft global network. There's no public internet access.
- Private Link is global and there are no regional restrictions. You can connect privately to services running in other Azure regions.
- Services delivered on Azure can be brought into your private virtual network by mapping your network to a private endpoint.
- Private Link can privately deliver your own services in your customer's virtual networks.
- All traffic to the service can be routed through the private endpoint. No gateways, NAT devices, Azure ExpressRoute or VPN connections, or public IP addresses are required.

The following illustration demonstrates a network routing configuration with Azure Private Link. The service connects to a network security group (NSG) private endpoint by using Azure SQL Database. This configuration prevents a direct connection.



Things to consider when using Azure Private Link

There are many benefits to working with Azure Private Link. Review the following points and consider how you can implement the service for your scenarios.

- Consider private connectivity to services on Azure. Connect privately to services running in other Azure regions. Traffic remains on the Microsoft network with no public internet access.
- Consider integration with on-premises and peered networks. Access private endpoints over private peering or VPN tunnels from on-premises or peered virtual networks. Microsoft hosts the traffic, so you don't need to set up public peering or use the internet to migrate your workloads to the cloud.
- Consider protection against data exfiltration for Azure resources. Map private endpoints to Azure PaaS resources. When there's a security incident within your network, only the mapped resources are accessible. This implementation eliminates the threat of data exfiltration.
- Consider services delivered directly to customer virtual networks. Privately consume Azure PaaS, Microsoft partner, and your own services in your virtual networks on Azure. Private Link works across Azure Active Directory (Azure AD) tenants to help unify your experience across services. Send, approve, or reject requests directly without permissions or role-based access controls.

Answer the following questions

Choose the best response for each of the following questions. Then select Check your answers.

1. Which statement best describes Azure routing? *

- Administrators can create system routes.
- When the next hop type is *none*, traffic is dropped.
- ✓ Correct. Traffic routed to the *none* next hop type is dropped and not routed outside the subnet.
- Azure gateways are needed to route traffic between subnets

2. What's a valid next hop type? *

- Load Balancer
- ExpressRoute
- Internet

✓ Correct. The valid next hop choices are virtual appliance, virtual network gateway, virtual network, internet, and none.

3. How can you extend the company's private address space with direct connections to Azure resources? *

- Virtual network endpoints
- ✓ Correct. Virtual network endpoints extend the private address space in Azure. Endpoints restrict the flow of traffic. As service endpoints are created, Azure creates routes in the route table to direct the traffic.
- User-defined routes
- ✗ Incorrect. User-defined routes are created so Azure virtual appliances can handle the traffic both between subnets and to the internet.
- Virtual appliances

Check your knowledge

1. What are some of the typical components involved in a network design? *

- A dedicated leased line
- A VM, subnet, firewall, and load balancer

✓ Typical components involved in a network design do include a VM, subnet, firewall, and load balancer.

- A dedicated network security group

2. Which of the following IP address ranges is routable over the internet? *

- 10.0.0.0 to 10.255.255.255
- 215.11.0.0 to 215.11.255.255

✓ Correct, this address range is routable over the internet.

- 172.16.0.0 to 172.31.255.255
- 192.168.0.1 to 192.168.255.255

Check your knowledge

1. Which of the following resources can you assign a public IP address to? *

- A virtual machine

✓ Correct. You can assign public IP addresses to virtual machines.

- Azure Data Lake
- Azure Key Vault

2. What must a virtual machine have to communicate with the other resources in the same virtual network? *

- Load balancer
- Network security group
- Network interface

✓ Correct. An IP address is assigned to a network interface, which is assigned to a virtual machine.

Network virtual appliance (NVA)

What is an NVA?

200 XP

7 minutes

A network virtual appliance (NVA) is a virtual appliance that consists of various layers like:

- a firewall
- a WAN optimizer
- application-delivery controllers
- routers
- load balancers
- IDS/IPS
- proxies

You can deploy NVAs chosen from providers in Azure Marketplace. Such providers include Cisco, Check Point, Barracuda, Sophos, WatchGuard, and SonicWall. You can use an NVA to filter traffic inbound to a virtual network, to block malicious requests, and to block requests made from unexpected resources.

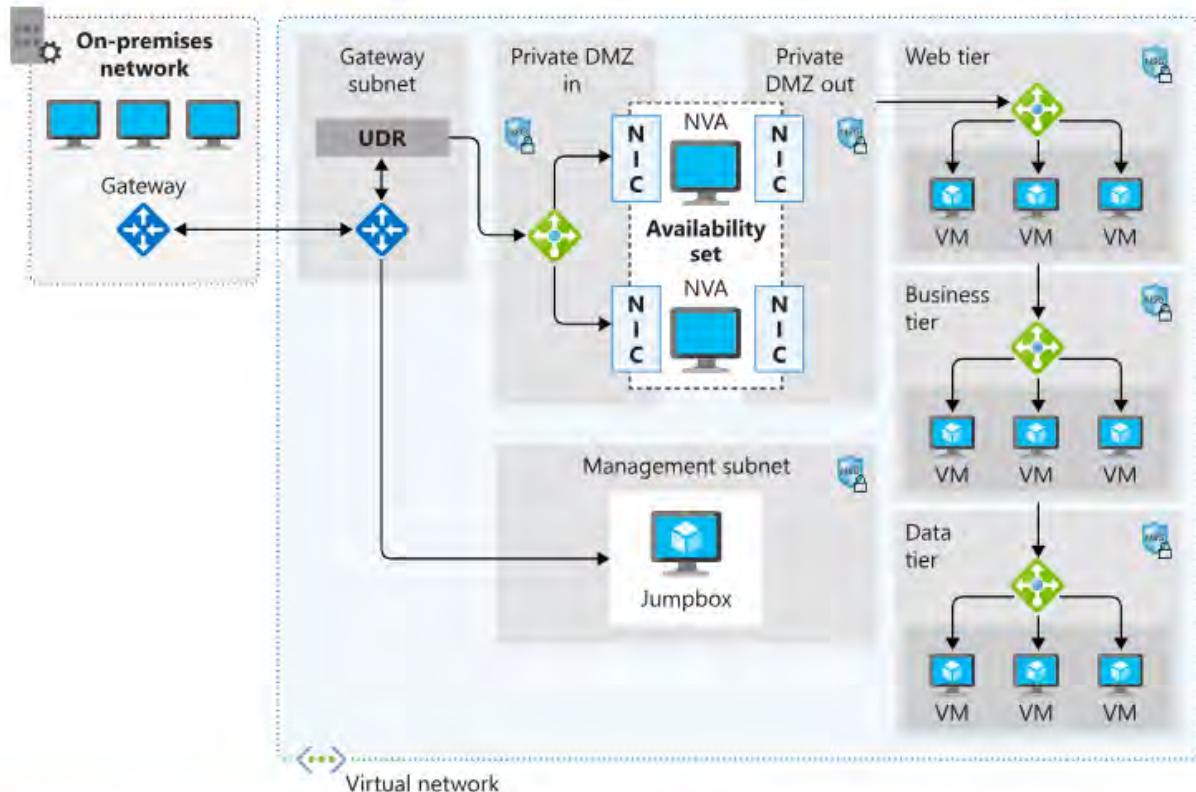
In the retail-organization example scenario, you must work with the security and network teams. You want to implement a secure environment that scrutinizes all incoming traffic and blocks unauthorized traffic from passing on to the internal network. You also want to secure both virtual-machine networking and Azure-services networking as part of your company's network-security strategy.

Your goal is to prevent unwanted or unsecured network traffic from reaching key systems.

As part of the network-security strategy, you must control the flow of traffic within your virtual network. You also must learn the role of an NVA and the benefit of using an NVA to control traffic flow through an Azure network.

Network virtual appliance

Network virtual appliances (NVAs) are virtual machines that control the flow of network traffic by controlling routing. You'll typically use them to manage traffic flowing from a perimeter-network environment to other networks or subnets.



You can deploy firewall appliances into a virtual network in different configurations. You can put a firewall appliance in a perimeter-network subnet in the virtual network or if you want more control of security, implement a microsegmentation approach.

With the microsegmentation approach, you can create dedicated subnets for the firewall and then deploy web applications and other services in other subnets. All traffic is routed through the firewall and inspected by the NVAs. You'll enable forwarding on the virtual-appliance network interfaces to pass traffic that is accepted by the appropriate subnet.

Microsegmentation lets the firewall inspect all packets at OSI Layer 4 and, for application-aware appliances, Layer 7. When you deploy an NVA to Azure, it acts as a router that forwards requests between subnets on the virtual network.

Some NVAs require multiple network interfaces. One network interface is dedicated to the management network for the appliance. Additional network interfaces manage and control the traffic processing. After you've deployed the NVA, you can then configure the appliance to route the traffic through the proper interface.

1. What is the main benefit of using a network virtual appliance? *

- To control outbound access to the internet.
- To load balance incoming traffic from the internet across multiple Azure Virtual machines and across two regions for DR purposes.
- To control incoming traffic from the perimeter network and allow only traffic that meets security requirements to pass through.

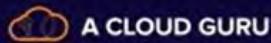
✓ This is the correct answer. A network virtual appliance acts like a firewall. It checks all inbound and outbound traffic, and it secures your environment by allowing or denying the traffic.
- To control who can access Azure resources from the perimeter network.

2. How might you deploy a network virtual appliance? *

- You can configure a Windows virtual machine and enable IP forwarding after routing tables, user-defined routes, and subnets have been updated. Or you can use a partner image from Azure Marketplace.

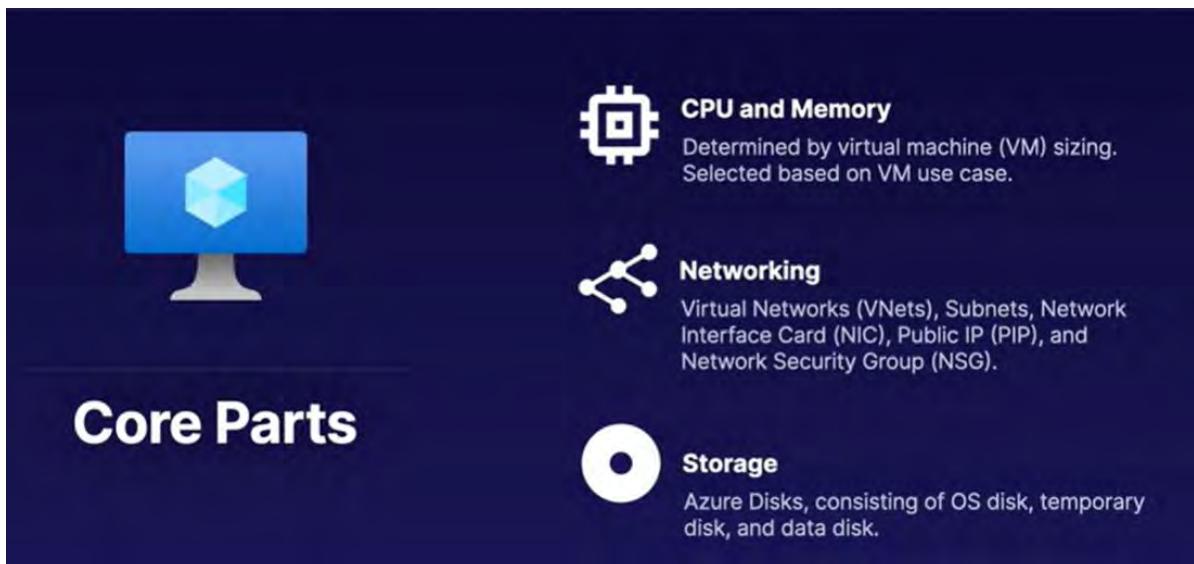
✓ This is the correct answer. Customers often create network virtual appliances. And you can download many appliances from Azure Marketplace.
- Using Azure CLI, deploy a Linux virtual machine in Azure, connect this virtual machine to your production virtual network, and assign a public IP address.
- Using the Azure portal, deploy a Windows 2016 Server instance. Next, using Azure Application Gateway add the Windows 2016 Server instance as a target endpoint.
- Download a virtual appliance from Azure Marketplace and configure the appliance to connect to the production and perimeter networks.

✗ This answer is incorrect. Simply installing a virtual appliance and connecting it to your networks forms only half of the solution and won't control the flow of traffic.



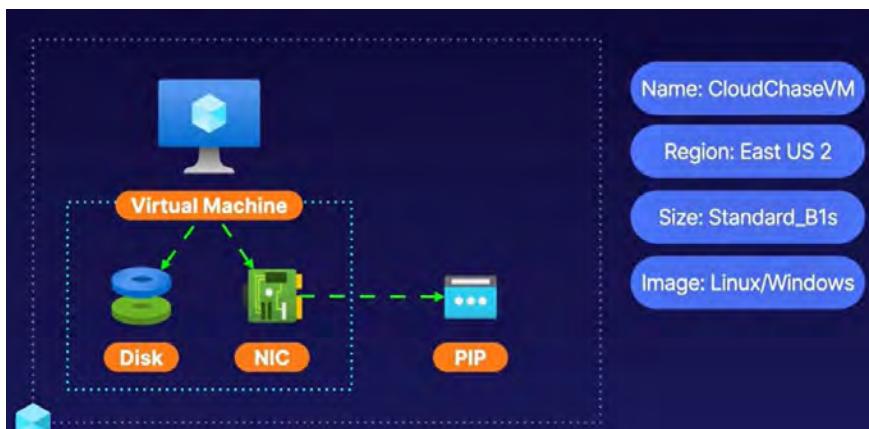
What is an Azure Virtual Machine?

- ✔ Scalable cloud computing resource offered as Infrastructure as a Service (IaaS).
- ✔ Includes CPU, memory, storage, and networking resources.
- ✔ Can be created from the Azure Portal, Azure CLI, or PowerShell.



Keeping VM Workloads in the Family

VM Family Type	Description
General Purpose	Balanced CPU-to-memory. Best for testing, development, or for small to medium workloads.
Compute Optimized	High CPU-to-memory. Good for medium traffic web servers, network appliances, batch processing, and app servers.
Memory Optimized	High memory-to-CPU. Works well for relational databases, caching, and in-memory analytics.
Storage Optimized	High disk throughput and I/O. Good for Big Data, SQL, NoSQL, and data warehousing. Works well for Online Transactional Processing (OLTP) databases.
GPU	Specialized for heavy graphic rendering and video editing. Works well for artificial intelligence (AI) training and deep learning.
HPC	Fastest and most powerful. Great for intensive workloads like large scale geophysics and advanced mathematics/sciences.



Intended Purposes

1

Linux/Windows Compute

Deploy Linux/Windows virtual machines using Azure VM's IaaS model.

2

Migrate Workloads

Migrate compute workloads to Azure. For example, move web servers to Azure VMs.

3

Cloud Computing Solutions

Azure VM workloads with specific configurations and additional resources can provide solutions with high availability, fault tolerance, scalability, and elasticity.

Key Components

CPU/Memory



Sizing determines CPU and memory

Networking



VMs use VNets, NICs, and NSGs to determine connectivity

Storage



VMs use Azure Disks to store OS, non-persistent, and persistent data

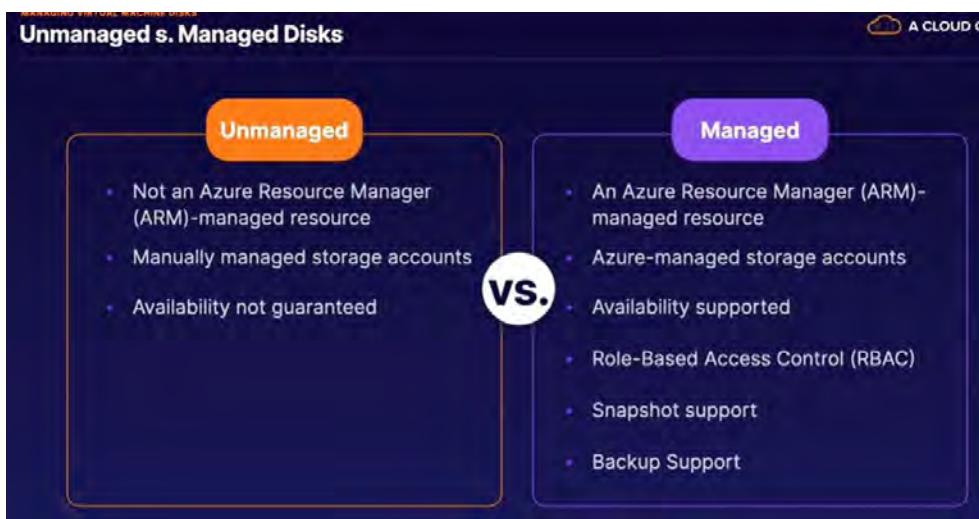
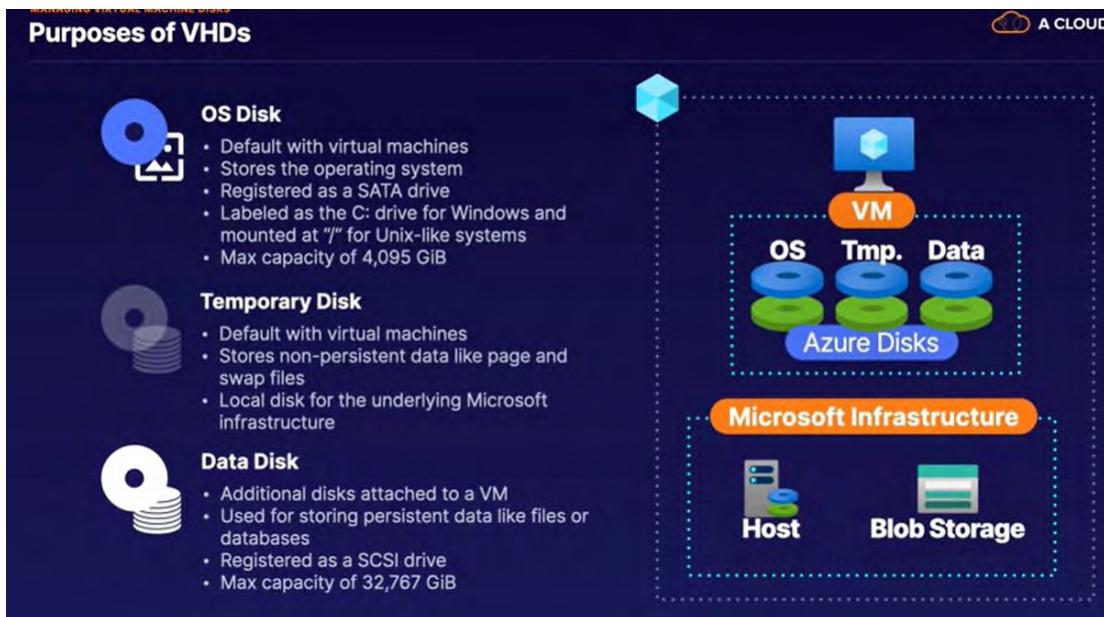
Managing virtual machine disks

Virtual Hard Disks (VHDs)

A file representation of what is found on a hard disk.

Virtual machines (VMs) use VHDs to store OS, apps, and data. VHDs utilize the underlying Microsoft storage infrastructure. They are stored as page blobs in the blob service.





Major Disk Types

Disk Type	Scenario
Ultra Disk (SSD)	I/O-intensive workloads like top tier Online Transactional Processing (OLTP), any transaction-heavy workloads. (Only used as a data disk.)
Premium (SSD)	Production and performance workloads.
Standard (SSD)	Web servers, light enterprise applications, and dev/test workloads.
Standard (HDD)	Backup, non-critical workloads.

Disk Encryption at Rest for Defense in Depth

1 Storage Service Encryption (SSE)

- Encryption of physical disks in the data center
- Built into Azure platform

2 Azure Disk Encryption (ADE)

- Optional encryption of the VHDs
- Ensures a disk is only accessible by the VM that owns the disk
- OS tools like BitLocker and DM-Crypt

Things to know about Azure Virtual Machines

Consider the following characteristics of Azure Virtual Machines.

- Azure Virtual Machines is the basis of the Azure infrastructure as a service (IaaS) model. IaaS is an instant computing infrastructure, provisioned and managed over the internet.
- A virtual machine provides its own operating system, storage, and networking capabilities, and can run a wide range of applications.
- You can implement multiple virtual machines, and configure each machine with different software and settings to support separate operation scenarios, such as development, testing, and deployment.
- You can use virtual machines to quickly scale up and down with demand and pay only for what you use.
- The responsibilities associated with configuring and maintaining virtual machines is shared between Microsoft and the customer. The following chart shows how the responsibilities are handled across the IaaS (virtual machines), PaaS, SaaS, and on-premises offerings.



Things to consider when using IaaS and virtual machines

Let's look at some scenarios for working with IaaS and virtual machines. Think about how you can implement virtual machines in Azure.

- Consider test and development. Teams can quickly set up and dismantle test and development environments, bringing new applications to market faster. IaaS and virtual machines make it quick and economical to scale up dev-test environments up and down.
- Consider website hosting. Running websites by using IaaS and virtual machines can be less expensive than traditional web hosting.
- Consider storage, backup, and recovery. Virtual machines let organizations avoid the expense for storage and complexity of storage management. Recovery typically requires a skilled staff to manage data and meet legal and compliance requirements. IaaS is useful for handling unpredictable demand and steadily growing storage needs. You can simplify planning and management of backup and recovery systems.
- Consider high-performance computing. Virtual machines enable high-performance computing (HPC) on supercomputers, computer grids, or computer clusters. HPC helps solve complex problems involving millions of variables or calculations. You can support scenarios such as earthquake and protein folding simulations, climate and weather predictions, financial modeling, and evaluating product designs.
- Consider big data analysis. Big data is a popular term for massive data sets that contain potentially valuable patterns, trends, and associations. Mining data sets to locate or tease out these hidden patterns requires a huge amount of processing power, which IaaS economically provides.
- Consider extended datacenters. Add capacity to your datacenter by adding virtual machines in Azure. Avoid the costs of physically adding hardware or space to your physical location. Connect your physical network to the Azure cloud network seamlessly.

Plan virtual machines

✓ 100 XP

5 minutes

Before you create an Azure virtual machine, it's helpful to make a plan for the machine configuration. You need to consider your preferences for several options, including the machine size and location, storage usage, and associated costs.

Things to know about configuring virtual machines

Let's walk through a checklist of things you need to consider when configuring a virtual machine.

- Start with the network.
- Choose a name for the virtual machine.
- Decide the location for the virtual machine.
- Determine the size of the virtual machine.
- Review the pricing model and estimate your costs.
- Identify which Azure Storage to use with the virtual machine.
- Select an operating system for the virtual machine.

Network configuration

Virtual networks are used in Azure to provide private connectivity between Azure Virtual Machines and other Azure services. Virtual machines and services that are part of the same virtual network can access one another. By default, services outside the virtual network can't connect to services within the virtual network. You can, however, configure the network to allow access to the external service, including your on-premises servers.

Network addresses and subnets aren't trivial to change after they're configured. If you plan to connect your private company network to the Azure services, make sure you consider the topology before you put any virtual machines into place.

Virtual machine name

The virtual machine name is used as the computer name, which is configured as part of the operating system. You can specify a name with up to 15 characters on a Windows virtual machine and 64 characters on a Linux virtual machine.

The virtual machine name also defines a manageable Azure resource, and it's not trivial to change later. You should choose names that are meaningful and consistent, so you can easily identify what the virtual machine does. A good convention uses several of the following elements in the machine name:

Name element	Examples	Description
Environment or purpose	dev (development), prod (production), QA (testing)	A portion of the name should identify the environment or purpose for the machine.
Location	uw (US West), je (Japan East), ne (North Europe)	Another portion of the name should specify the region where the machine is deployed.
Instance	1, 02, 005	For multiple machines that have similar names, include an instance number in the name to differentiate the machines in the same category.
Product or service	Outlook, SQL, AzureAD	A portion of the name can specify the product, application, or service that the machine supports.
Role	security, web, messaging	A portion of the name can specify what role the machine supports within the organization.

Let's consider how to name the first development web server for your company that's hosted in the US South Central location. In this scenario, you might use the machine name devusc-webvm01. dev stands for development and usc identifies the location. web indicates the machine as a web server, and the suffix 01 shows the machine is the first in the configuration.

Virtual machine location

Azure has datacenters all over the world filled with servers and disks. These datacenters are grouped into geographic regions like West US, North Europe, Southeast Asia, and so on. The datacenters provide redundancy and availability.

Each virtual machine is in a region where you want the resources like CPU and storage to be allocated. The regional location lets you place your virtual machines as close as possible to your users. The location of the machine can improve performance and ensure you meet any legal, compliance, or tax requirements.

There are two other points to consider about the virtual machine location.

- The machine location can limit your available options. Each region has different hardware available, and some configurations aren't available in all regions.
- There are price differences between locations. To find the most cost-effective choice, check for your required configuration in different regions.

Virtual machine size

Azure offers different memory and storage options for different virtual machine sizes. The best way to determine the appropriate machine size is to consider the type of workload your machine needs to run. Based on the workload, you can choose from a subset of available virtual machine sizes.

Azure Storage

Azure Managed Disks handle Azure storage account creation and management in the background for you. You specify the disk size and the performance tier (Standard or Premium). Azure creates and manages the disk. As you add disks or scale the virtual machine up and down, you don't have to worry about the storage being used.

Virtual machine pricing options

A subscription is billed two separate costs for every virtual machine: *compute* and *storage*. By separating these costs, you can scale them independently and only pay for what you need.

- Compute expenses are priced on a per-hour basis but billed on a per-minute basis. If the virtual machine is deployed for 55 minutes, you're charged for only 55 minutes of usage. You're not charged for compute capacity if you stop and deallocate the virtual machine. The hourly price varies based on the virtual machine size and operating system you select. For the compute costs, you're able to choose from two payment options:
 - Consumption-based: With the consumption-based option, you pay for compute capacity by the second. You're able to increase or decrease compute capacity on demand and start or stop at any time. Use consumption-based pricing if you run applications with short-term or unpredictable workloads that can't be interrupted. An example scenario is if you're doing a quick test or developing an app in a virtual machine.
 - Reserved Virtual Machine Instances: The Reserved Virtual Machine Instances (RI) option is an advance purchase of a virtual machine for one or three years in a specified region. The commitment is made up front, and in return, you get up to 72% price savings compared to pay-as-you-go pricing. RIs are flexible and can easily be exchanged or returned for an early termination fee. Use this option if the virtual machine has to run continuously, or you need budget predictability, and you can commit to using the virtual machine for at least a year.
- Storage costs are charged separately for the Azure Storage used by the virtual machine. The status of the virtual machine has no relation to the Azure Storage charges that are incurred. You're always charged for any Azure Storage used by the disks.

Operating system

Azure provides various operating system images that you can install into the virtual machine, including several versions of Windows and flavors of Linux. Azure bundles the cost of the operating system license into the price.

- If you're looking for more than just base operating system images, you can search Azure Marketplace. There are various install images that include not only the operating system but popular software tools, such as WordPress. The image stack consists of a Linux server, Apache web server, a MySQL database, and PHP. Instead of setting up and configuring each component, you can install an Azure Marketplace image and get the entire stack all at once.
- If you don't find a suitable operating system image, you can create your own disk image. Your disk image can be uploaded to Azure Storage and used to create an Azure virtual machine. Keep in mind that Azure only supports 64-bit operating systems.

Things to know about virtual machine sizes

The best way to determine the appropriate virtual machine size is to consider the type of workload your virtual machine needs to run. Based on the workload, you can choose from a subset of available virtual machine sizes.

The following table shows size classifications for Azure Virtual Machines workloads and recommended usage scenarios.

Classification	Description	Scenarios
General purpose	General-purpose virtual machines are designed to have a balanced CPU-to-memory ratio.	- Testing and development - Small to medium databases - Low to medium traffic web servers
Compute optimized	Compute optimized virtual machines are designed to have a high CPU-to-memory ratio.	- Medium traffic web servers - Network appliances - Batch processes - Application servers
Memory optimized	Memory optimized virtual machines are designed to have a high memory-to-CPU ratio.	- Relational database servers - Medium to large caches - In-memory analytics
Storage optimized	Storage optimized virtual machines are designed to have high disk throughput and I/O.	- Big Data - SQL and NoSQL databases - Data warehousing - Large transactional databases
GPU	GPU virtual machines are specialized virtual machines targeted for heavy graphics rendering and video editing. Available with single or multiple GPUs.	- Model training - Inferencing with deep learning
High performance computes	High performance compute offers the fastest and most powerful CPU virtual machines with optional high-throughput network interfaces (RDMA).	- Workloads that require fast performance - High traffic networks

Resizing virtual machines

Azure allows you to change the virtual machine size when the existing size no longer meets your needs. You can resize a virtual machine if your current hardware configuration is allowed in the new size. This option provides a fully agile and elastic approach to virtual machine management.

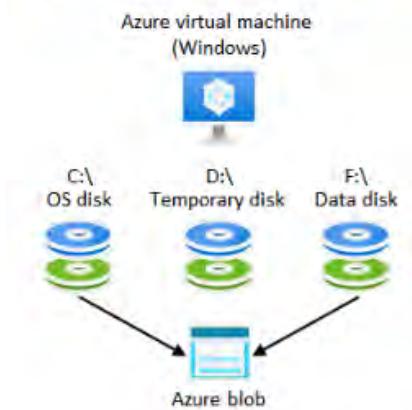
When you stop and deallocate the virtual machine, you can select any size available in your region.

ⓘ Important

Be cautious when resizing production virtual machines. Resizing a machine might require a restart that can cause a temporary outage or change configuration settings such as the IP address.

Things to know about virtual machine storage and disks

All Azure virtual machines have at least two disks: an operating system disk and a temporary disk. Virtual machines can also have one or more data disks. All disks are stored as virtual hard disks (VHDs). A VHD is like a physical disk in an on-premises server but, virtualized.



Operating system disk

Every virtual machine has one attached operating system disk. The OS disk has a pre-installed operating system, which is selected when the virtual machine is created. The OS disk is registered as a SATA drive (Serial Advanced Technology Attachment) and labeled as the c: drive by default.

Temporary disk

Data on a temporary disk might be lost during a maintenance event or when you redeploy a virtual machine. During a standard reboot of the virtual machine, the data on the temporary drive should persist. However, there are cases where the data might not persist, such as moving to a new host. Therefore, any data on the temporary drive shouldn't be data that's critical to the system.

- On Windows virtual machines, the temporary disk is labeled as the d: drive by default. This drive is used for storing the pagefile.sys file.
- On Linux virtual machines, the temporary disk is typically /dev/sdb. This disk is formatted and mounted to /mnt by the Azure Linux Agent.

ⓘ Important

Don't store data on the temporary disk. This disk provides temporary storage for applications and processes and is intended to only store data like page or swap files.

Data disks

A data disk is a managed disk that's attached to a virtual machine to store application data, or other data you need to keep. Data disks are registered as SCSI drives and are labeled with a letter you choose. The size of a virtual machine determines how many data disks you can attach and the type of storage you can use to host the data disks.

Things to consider when choosing storage for your virtual machines

Review the following considerations about using Azure Storage and Azure Managed Disks with your virtual machines.

- Consider Azure Premium Storage. You can choose Premium Storage to gain high-performance, low-latency disk support for your virtual machines with input/output (I/O)-intensive workloads. Virtual machine disks that use Premium Storage store data on solid-state drives (SSDs). To take advantage of the speed and performance of premium storage disks, you can migrate existing virtual machine disks to Premium Storage.
- Consider multiple Storage disks. In Azure, you can attach several Premium Storage disks to a virtual machine. Using multiple disks gives your applications up to 256 TB of storage per virtual machine. With Premium Storage, your applications can achieve 80,000 I/O operations per second (IOPS) per virtual machine, and a disk throughput of up to 2,000 megabytes per second (MB/s) per virtual machine. Read operations completed with Premium Storage yield low latencies.
- Consider managed disks. An Azure-managed disk is a VHD. Azure-managed disks are stored as page blobs, which are a random IO storage object in Azure. The disk is described as *managed* because it's an abstraction over page blobs, blob containers, and Azure storage accounts. With managed disks, you provision the disk, and Azure takes care of the rest. When you choose to use Azure-managed disks with your workloads, Azure creates and manages the disk for you. The available types of disks are Ultra Solid State Drives (SSD), Premium SSD, Standard SSD, and Standard Hard Disk Drives (HDD).

Note

Managed disks are required for the single instance virtual machine SLA.

- Consider migrating to Premium Storage. For the best performance for your application, we recommend that you migrate any virtual machine disk that requires high IOPS to Premium Storage. If your disk doesn't require high IOPS, you can help limit costs by keeping it in standard Azure Storage.

1. Which virtual machine is best for running a network appliance? *

Memory-optimized virtual machine

✗ Incorrect. Memory-optimized virtual machines are better for large in-memory business critical workloads that require massive parallel compute power.

Compute-optimized virtual machine

✓ Correct. Compute-optimized virtual machines are designed to have a high CPU-to-memory ratio. These virtual machines are suitable for medium traffic web servers, network appliances, batch processes, and application servers.

Storage-optimized virtual machine

2. For the security requirements, how can you connect to Azure Linux virtual machines and install software? *

Configure a guest configuration on the virtual machine

Create a custom script extension

Configure Azure Bastion.

✓ Correct. Azure Bastion is a fully platform-managed PaaS service provisioned inside a virtual network. Azure Bastion provides secure and seamless RDP and SSH connectivity to virtual machines. The access uses the Azure portal and SSL.

3. What effect do the default network security settings have on a new virtual machine? *

Outbound requests are allowed. Inbound traffic is allowed only from within the virtual network.

✓ Correct. Outbound requests are considered low risk, so they're allowed by default. Inbound traffic from within the virtual network is allowed.

No outbound and inbound requests are allowed.

✗ Incorrect. Outbound requests are allowed by default.

There are no restrictions. All outbound and inbound requests are allowed.

Configuring Virtual Machine Availability and Scale

Purpose of Availability Sets



✓ Protect redundant VMs

✓ Protect against underlying host failures

CONFIGURING VIRTUAL MACHINE AVAILABILITY AND SCALE SETS

Virtual Machine Availability Sets

A CLOUD

Fault Domain (FD)
Underlying host failure, such as power or network outages.
(Max FD: 3)

Update Domain (UD)
Logical grouping of infrastructure for maintenance/updates.
(Max UD: 20)

FD 1 **FD 2**

Para poder agregar un vm a un availability set es necesario crearla después del availability y no antes

An availability set is a logical grouping of VMs that allows Azure to understand how your application is built to provide for redundancy and availability. We recommend that two or more VMs are created within an availability set to provide for a highly available application and to meet the [99.95% Azure SLA](#). There is no cost for the Availability Set itself, you only pay for each VM instance that you create.

Each availability set can be configured with up to three fault domains and twenty update domains

A rebooted update domain is given 30 minutes to recover before maintenance is initiated on a different update domain.

Purpose of Virtual Machine Scale Sets

- Simplify scaling configurations
- Save costs by aligning usage with demand
- Scale to meet demand of traffic



CONFIGURING VIRTUAL MACHINE AVAILABILITY AND SCALE SETS

Virtual Machine Scale Set Components

A CLOUD GURU

VM Definition	VM Definition
Region	Define VM size, OS, NICs, storage, etc.
Size	
Image	
Name	

Scaling Definition	Autoscaling Definition
Default	Define scaling actions, scaling in/out based on condition met (e.g. If CPU utilization > 80% then +1 VM).
Condition: CPU 75%	
Action: +1 VM	

Scale-In Policy
Delete VMs by priority as scaling-in operations occur.

Scale-In policy

Default - Balance across availability zones and fault domains, then delete VM with highest instance ID

Configure the order in which virtual machines are deleted during a scale-in operation. Newest VM - Balance across availability zones, then delete the newest created VM

Learn more about scale-in policies. ↗

Oldest VM - Balance across availability zones, then delete the oldest created VM

Scale-in policy

Default - Balance across availability zones and fault domains, then delete ...

Things to know about maintenance planning

An availability plan for Azure virtual machines needs to include strategies for unplanned hardware maintenance, unexpected downtime, and planned maintenance. As you review the following scenarios, think about how these scenarios can impact the example company website.

- An unplanned hardware maintenance event occurs when the Azure platform predicts that the hardware or any platform component associated to a physical machine is about to fail. When the platform predicts a failure, it issues an unplanned hardware maintenance event. Azure uses Live Migration technology to migrate your virtual machines from the failing hardware to a healthy physical machine. Live Migration is a virtual machine preserving operation that only pauses the virtual machine for a short time, but performance might be reduced before or after the event.
- Unexpected downtime occurs when the hardware or the physical infrastructure for your virtual machine fails unexpectedly. Unexpected downtime can include local network failures, local disk failures, or other rack level failures. When detected, the Azure platform automatically migrates (heals) your virtual machine to a healthy physical machine in the same datacenter. During the healing procedure, virtual machines experience downtime (reboot) and in some cases loss of the temporary drive.
- Planned maintenance events are periodic updates made by Microsoft to the underlying Azure platform to improve overall reliability, performance, and security of the platform infrastructure that your virtual machines run on. Most of these updates are performed without any impact to your virtual machines or Cloud Services.

ⓘ Note

Microsoft doesn't automatically update your virtual machine operating system or other software. You have complete control and responsibility for those updates. However, the underlying software host and hardware are periodically patched to ensure reliability and high performance.

Create availability sets

✓ 100 XP

2 minutes

An availability set is a logical feature you can use to ensure a group of related virtual machines are deployed together. The grouping helps to prevent a single point of failure from affecting all of your machines. The grouping ensures that not all of the machines are upgraded at the same time during a host operating system upgrade in the datacenter.

Things to know about availability sets

Let's review some characteristics of availability sets.

- All virtual machines in an availability set should perform the identical set of functionalities.
- All virtual machines in an availability set should have the same software installed.
- Azure ensures that virtual machines in an availability set run across multiple physical servers, compute racks, storage units, and network switches.

If a hardware or Azure software failure occurs, only a subset of the virtual machines in the availability set are affected. Your application stays up and continues to be available to your customers.

- You can create a virtual machine and an availability set at the same time.

A virtual machine can only be added to an availability set when the virtual machine is created. To change the availability set for a virtual machine, you need to delete and then recreate the virtual machine.

- You can build availability sets by using the Azure portal, Azure Resource Manager (ARM) templates, scripting, or API tools.
- Microsoft provides robust Service Level Agreements (SLAs) for Azure virtual machines and availability sets. For details, see [SLA for Azure Virtual Machines](#).

Note

Adding your virtual machines to an availability set won't protect your applications from operating system or application-specific failures. You'll need to explore other disaster recovery and backup techniques to provide application-level protection.

Things to consider when using availability sets

Availability sets are an essential capability when you want to build reliable cloud solutions. In your planning for availability sets, keep the following general principles in mind:

- Consider redundancy. To achieve redundancy in your configuration, place multiple virtual machines in an availability set.
- Consider separation of application tiers. Each application tier exercised in your configuration should be located in a separate availability set. The separation helps to mitigate single point of failure on all machines.
- Consider load balancing. For high availability and network performance, create a load-balanced availability set by using Azure Load Balancer. Load Balancer distributes incoming traffic across working instances of services that are defined in your load-balanced availability set.
- Consider managed disks. You can use Azure managed disks with your Azure virtual machines in availability sets for block-level storage.

Review update domains and fault domains

100 XP

2 minutes

Azure Virtual Machine Availability Sets implements two node concepts to help Azure maintain high availability and fault tolerance when deploying and upgrading applications: *update domains* and *fault domains*. Each virtual machine in an availability set is placed in one update domain and one fault domain.

Things to know about update domains

An update domain is a group of nodes that are upgraded together during the process of a service upgrade (or *rollout*). An update domain allows Azure to perform incremental or rolling upgrades across a deployment. Here are some other characteristics of update domains.

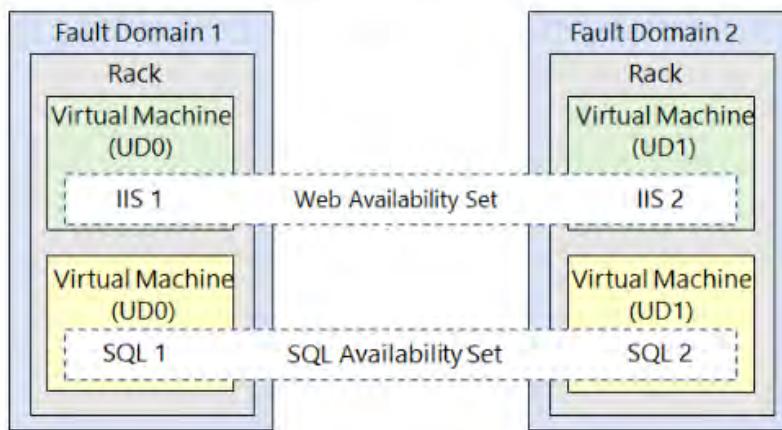
- Each update domain contains a set of virtual machines and associated physical hardware that can be updated and rebooted at the same time.
- During planned maintenance, only one update domain is rebooted at a time.
- By default, there are five (non-user-configurable) update domains.
- You can configure up to 20 update domains.

Things to know about fault domains

A fault domain is a group of nodes that represent a physical unit of failure. Think of a fault domain as nodes that belong to the same physical rack.

- A fault domain defines a group of virtual machines that share a common set of hardware (or switches) that share a single point of failure. An example is a server rack serviced by a set of power or networking switches.
- Two fault domains work together to mitigate against hardware failures, network outages, power interruptions, or software updates.

Let's look at a scenario with two fault domains that have two virtual machines each. The virtual machines in each fault domain are contained in different availability sets. The web availability set contains two virtual machines with one machine from each fault domain. The SQL availability set contains two different virtual machines with one from each fault domain.



Review availability zones

✓ 100 XP

2 minutes

Availability zones are a high-availability offering that protects your applications and data from datacenter failures. An availability zone in an Azure region is a combination of a fault domain and an update domain.

Consider a scenario where you create three or more virtual machines across three zones in an Azure region. Your virtual machines are effectively distributed across three fault domains and three update domains. The Azure platform recognizes this distribution across update domains to make sure that virtual machines in different zones aren't updated at the same time.

You can use availability zones to build high-availability into your application architecture by colocating your compute, storage, networking, and data resources within a zone and replicating in other zones.

Things to know about availability zones

Review the following characteristics of availability zones.

- Availability zones are unique physical locations within an Azure region.
- Each zone is made up of one or more datacenters that are equipped with independent power, cooling, and networking.
- To ensure resiliency, there's a minimum of three separate zones in all enabled regions.
- The physical separation of availability zones within a region protects applications and data from datacenter failures.
- Zone-redundant services replicate your applications and data across availability zones to protect against single-points-of-failure.

Things to consider when using availability zones

Azure services that support availability zones are divided into two categories.

Category	Description	Examples
Zonal services	Azure zonal services pin each resource to a specific zone.	- Azure Virtual Machines - Azure managed disks - Standard IP addresses
Zone-redundant services	For Azure services that are zone-redundant, the platform replicates automatically across all zones.	- Azure Storage that's zone-redundant - Azure SQL Database



To achieve comprehensive business continuity on Azure, build your application architecture by using a combination of availability zones with Azure region pairs.

Compare vertical and horizontal scaling

100 XP

2 minutes

A robust virtual machine configuration includes support for scalability. Scalability allows throughput for a virtual machine in proportion to the availability of the associated hardware resources. A scalable virtual machine can handle increases in requests without adversely affecting response time and throughput. For most scaling operations, there are two implementation options: *vertical* and *horizontal*.

Things to know about vertical scaling

Vertical scaling, also known as *scale up and scale down*, involves increasing or decreasing the virtual machine size in response to a workload. Vertical scaling makes a virtual machine more (scale up) or less (scale down) powerful.



Here are some scenarios where using vertical scaling can be advantageous:

- If you have a service built on a virtual machine that's under-utilized such as on the weekend, you can use vertical scaling to decrease the virtual machine size and reduce your monthly costs.
- You can implement vertical scaling to increase your virtual machine size to support larger demand without having to create extra virtual machines.

Implement Azure Virtual Machine Scale Sets

✓ 100 XP

2 minutes

Azure Virtual Machine Scale Sets are an Azure Compute resource that you can use to deploy and manage a set of identical virtual machines. When you implement Virtual Machine Scale Sets and configure all your virtual machines in the same way, you gain true *autoscaling*. Virtual Machine Scale Sets automatically increases the number of your virtual machine instances as application demand increases, and reduces the number of machine instances as demand decreases.

With Virtual Machine Scale Sets, you don't need to pre-provision your virtual machines. It's easier to build large-scale services that target large compute, big data, and containerized workloads. As workloads increase, more virtual machine instances can be added. As workloads decrease, virtual machines instances can be removed. The process of adding and removing machines can be manual or automated, or a combination of both.

Things to know about Azure Virtual Machine Scale Sets

Review the following characteristics of Azure Virtual Machine Scale Sets.

- All virtual machine instances are created from the same base operating system image and configuration. This approach lets you easily manage hundreds of virtual machines without extra configuration tasks or network management.
- Virtual Machine Scale Sets support the use of Azure Load Balancer for basic layer-4 traffic distribution, and Azure Application Gateway for more advanced layer-7 traffic distribution and SSL termination.
- You can use Virtual Machine Scale Sets to run multiple instances of your application. If one of the virtual machine instances has a problem, customers continue to access your application through another virtual machine instance with minimal interruption.
- Customer demand for your application might change throughout the day or week. To meet customer demand, Virtual Machine Scale Sets implements autoscaling to automatically increase and decrease the number of virtual machines.
- Virtual Machine Scale Sets support up to 1,000 virtual machine instances. If you create and upload your own custom virtual machine images, the limit is 600 virtual machine instances.

Things to know about horizontal scaling

Horizontal scaling, also referred to as *scale out and scale in*, is used to adjust the number of virtual machines in your configuration to support the changing workload. When you implement horizontal scaling, there's an increase (scale out) or decrease (scale in) in the number of virtual machine instances.



Things to consider when using vertical and horizontal scaling

Review the following considerations regarding vertical and horizontal scaling. Think about which implementation might be required to support your company website.

- **Consider limitations.** Generally speaking, horizontal scaling has fewer limitations than vertical scaling. A vertical scaling implementation depends on the availability of larger hardware, which quickly hits an upper limit and can vary by region. Vertical scaling also usually requires a virtual machine to stop and restart, which can temporarily limit access to applications or data.
- **Consider flexibility.** When operating in the cloud, horizontal scaling is more flexible. A horizontal scaling implementation allows you to run potentially thousands of virtual machines to manage changes in workload and throughput.
- **Consider reprovisioning.** Reprovisioning is the process of removing an existing virtual machine and replacing it with a new machine. A robust availability plan considers where reprovisioning might be required and plans for interruptions to service. If reprovisioning might be required, determine if any data needs to be maintained and migrated to the new machine.

- **Orchestration mode:** Choose how virtual machines are managed by the scale set. In flexible orchestration mode, you manually create and add a virtual machine of any configuration to the scale set. In uniform orchestration mode, you define a virtual machine model and Azure will generate identical instances based on that model.
- **Image:** Choose the base operating system or application for the VM.
- **VM Architecture:** Azure provides a choice of x64 or Arm64-based virtual machines to run your applications.
- **Run with Azure Spot discount:** Azure Spot offers unused Azure capacity at a discounted rate versus pay as you go prices. Workloads should be tolerant to infrastructure loss as Azure may recall capacity.
- **Size:** Select a VM size to support the workload that you want to run. The size that you choose then determines factors such as processing power, memory, and storage capacity. Azure offers a wide variety of sizes to support many types of uses. Azure charges an hourly price based on the VM's size and operating system.

Under the Advanced tab, you can also select the following:

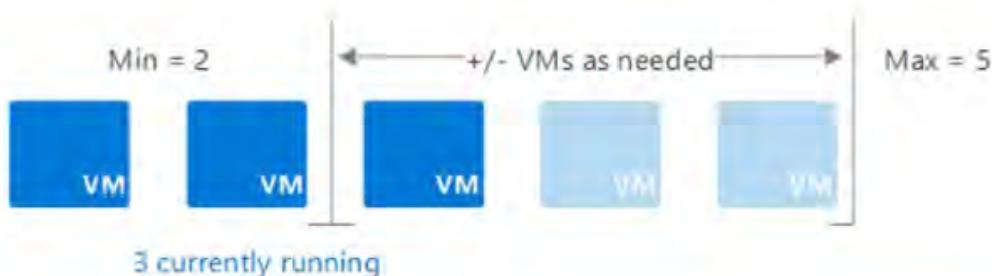
- **Enable scaling beyond 100 instances:** Identify your scaling allocation preference. If you select No, your Virtual Machine Scale Sets implementation is limited to one placement group with a maximum capacity of 100. If you select Yes, your implementation can span multiple placement groups with capacity up to 1,000. Selecting Yes also changes the availability characteristics of your implementation.
- **Spreading algorithm:** Microsoft recommends allocating Max spreading for your implementation. This approach provides the optimal spreading.

Implement autoscale

✓ 100 XP

2 minutes

An Azure Virtual Machine Scale Sets implementation can automatically increase or decrease the number of virtual machine instances that run your application. This process is known as *autoscaling*. Autoscaling allows you to dynamically scale your configuration to meet changing workload demands.



Autoscaling minimizes the number of unnecessary virtual machine instances that run your application when demand is low. Your customers continue to receive an acceptable level of performance as demand grows and more virtual machine instances are automatically added.

Things to consider when using autoscaling

Review the following considerations about autoscaling. Think about how this process can benefit your company website implementation.

- Consider automatic adjusted capacity. You can create autoscaling rules to define the acceptable performance for a positive customer experience. When the defined thresholds are met, the autoscale rules act to adjust the capacity of your Virtual Machine Scale Sets implementation.
 - Consider scale out. If your application demand increases, the load on the virtual machine instances in your implementation increases. If the increased load is consistent, rather than a brief demand, you can configure autoscale rules to increase the number of virtual machine instances in your implementation.
 - Consider scale in. On an evening or weekend, your application demand might decrease. If the decreased load is consistent over a period of time, you can configure autoscale rules to decrease the number of virtual machine instances in your implementation. The scale-in action reduces the cost to run your Virtual Machine Scale Sets implementation as you only run the number of instances required to meet the current demand.
 - Consider scheduled events. You can implement autoscaling and schedule events to automatically increase or decrease the capacity of your implementation at fixed times.
 - Consider overhead. Using Azure Virtual Machine Scale Sets with autoscaling reduces your management overhead to monitor and optimize the performance of your application.
-

Create a virtual machine scale set

Basics Disks Networking **Scaling** Management Health Advanced

Initial instance count * ⓘ

2

Scaling

Scaling policy ⓘ

Manual scaling
 Autoscaling

Minimum number of instances * ⓘ

1

Maximum number of instances * ⓘ

10

Scale out

CPU threshold (%) * ⓘ

75

Duration in minutes * ⓘ

10

Number of instances to increase by * ⓘ

1 ✓

Scale in

CPU threshold (%) * ⓘ

25

Number of instances to decrease by * ⓘ

1 ✓

Scale-In policy

Configure the order in which virtual machines are selected for deletion during a scale-in operation.

Scale-in policy

Default - Balance across availability zones and fault domains, then delete VM with highest instance ID

Newest VM - Balance across availability zones, then delete the newest created VM

Oldest VM - Balance across availability zones, then delete the oldest created VM

Scaling policy: Manual scale maintains a fixed instance count. Custom autoscale scales the capacity on any schedule, based on any metrics.

- **Minimum number of VMs:** Specify the minimum number of virtual machines that should be available when autoscaling is applied on your Virtual Machine Scale Sets implementation.
- **Maximum number of VMs:** Specify the maximum number of virtual machines that can be available when autoscaling is applied on your implementation.

Scale out

- **CPU threshold:** Specify the CPU usage percentage threshold to trigger the scale-out autoscale rule.
- **Duration in minutes:** Duration in minutes is the amount of time that Autoscale engine will look back for metrics. For example, 10 minutes means that every time autoscale runs, it will query metrics for the past 10 minutes. This delay allows your metrics to stabilize and avoids reacting to transient spikes.
- **Number of VMs to increase by:** Specify the number of virtual machines to add to your Virtual Machine Scale Sets implementation when the scale-out autoscale rule is triggered.

Scale in

- **Scale in CPU threshold:** Specify the CPU usage percentage threshold to trigger the scale-in autoscale rule.
- **Number of VMs to decrease by:** Specify the number of virtual machines to remove from your implementation when the scale-in autoscale rule is triggered.

Scale in policy: The scale-in policy feature provides users a way to configure the order in which virtual machines are scaled-in.

1. How can you ensure more virtual machines are deployed for the Admin team when the CPU is 75% consumed? *

- Manually increase the instance count.
- Change the CPU percentage to 50%.
- Enable the autoscale option.

✓ Correct. To meet the Admin team scenario requirements, enable the autoscale option so more virtual machines are created when the CPU is 75% consumed.

2. Which Virtual Machine Scale Sets feature can be configured to add more DevOps machines during peak production? *

- Schedule-based rules

✓ Correct. With schedule-based rules, administrators proactively schedule the scale set to deploy one or any number of instances.

- Autoscale

✗ Incorrect. Autoscale automatically increases or decreases the number of virtual machine instances that run the application. Is there a better solution based on demand?

- Metric-based rules

3. What types of scaling can you use to increase the CPU capacity for your existing Virtual Machine Scale Sets instances? *

- Horizontal scaling

- Vertical scaling

✓ Correct. Vertical scaling increases the *capacity* of existing instances within Azure Virtual Machine Scale Sets.

- Load balancing

Automating Virtual Machine deployment

```
Resource: "Virtual Machine" {
    Virtual Machine Properties: {
        Name: "VM1",
        Location: "East US",
        Size: "Standard_B1s",
        Storage: {
            OSImage: "Linux",
            DataDisk: "DataDisk1"
        },
        Network: {
            NIC: "NIC1"
        }
    }
}
```

1

Infrastructure as Code (IaC)

Text-based (declarative JSON) definition of Azure resources and resource configurations.

2

Deployment Consistency

Manage resource deployments using software deployment methodologies.

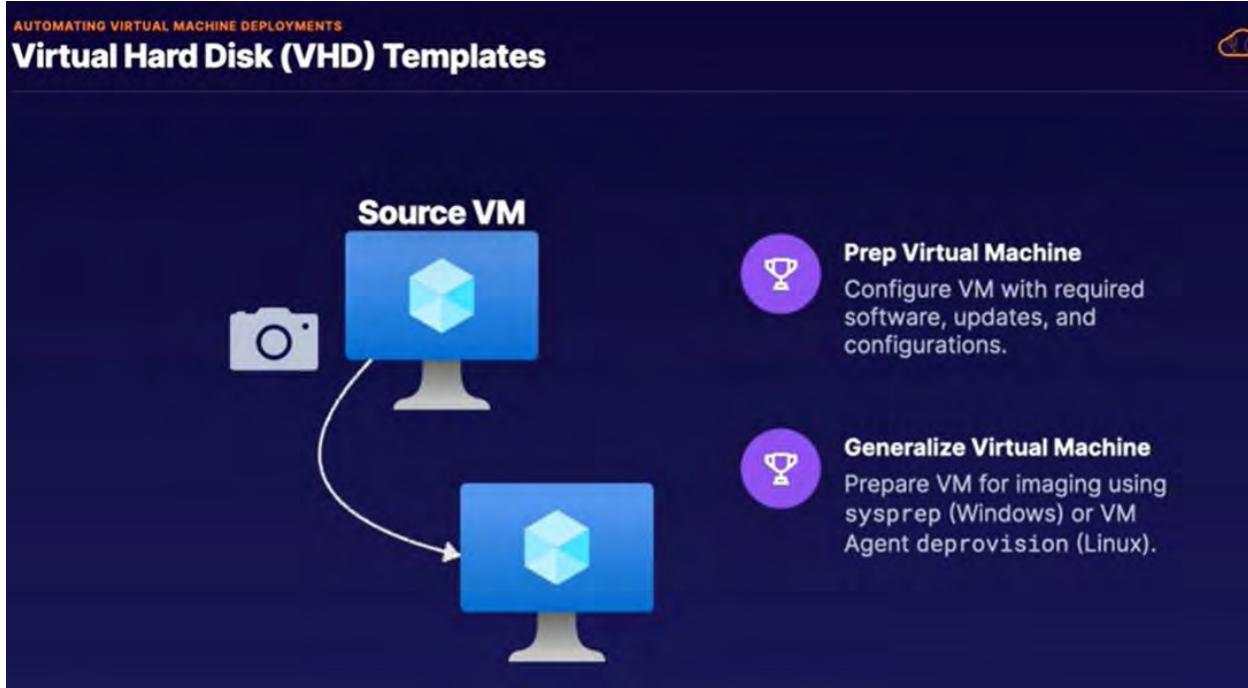
3

Automation

Automate resource deployments and provide modular approach to resource deployments.

Todo esto puede venir en un ARM template





Los pasos para crear una imagen de una vm son los siguientes:

```
# Generalize and Azure Linux VM
# NOTE: This exercise is completed using the commands via the ACG Azure Cloud Sandbox

# Login to VM
ssh <user>@<public_ip>

# Deprovision machine and delete machine specific files
sudo waagent -deprovision+user
exit

# Set variables
$rg = (Get-AzResourceGroup).ResourceGroupName
$myvm = az vm list --query [].name -o tsv

# Deallocate VM (may take a few minutes)
az vm deallocate ` 
    --resource-group $rg ` 
    --name $myvm

# Generalize VM
az vm generalize ` 
    --resource-group $rg ` 
    --name $myvm

# Create an Image of VM in same region as the source vm (may take a minute)
az image create ` 
    --resource-group $rg ` 
    --name myImage --source $myvm
```

Si nos vamos a los settings de una vm podemos generar un ARM template de esa vm

Exam TipsInstall NGINX on a Linux VM
Deployment with Cloud Init**ARM Templates**

Deploy VMs quickly and manage infrastructure using change control using Infrastructure as Code (IaC).

VHD Template

Create a golden image of VMs to easily deploy VMs with consistent software and configurations.

**Automate Management**

Manage VM deployments using custom data and manage VMs using extension scripts.

Así podemos instalar nginx en postdeploy de una vm con cloud_init

```
#cloud-config
packages_upgrade: true
packages:
  - nginx
```

Pasos para crear una imagen de un disco de una vm:

2. In the Azure Portal, click **All resources** and copy the name of the pre-provisioned resource group.

3. In the Cloud Shell, create a new variable:

```
$rg = "<RESOURCE_GROUP_NAME>"
```

4. In the Azure Portal, copy the name of the VM disk and create a new variable:

```
$diskname = "<VIRTUAL_MACHINE_DISK_NAME>"
```

5. Create a variable for **sasExpiryDuration**:

```
$sasExpiryDuration = "3600"
```

6. In the Azure Portal, copy the storage account name, and create a new variable:

```
$storageAccountName = "<STORAGE_ACCOUNT_NAME>"
```

7. In the Azure Portal, copy the storage account key for **key1**, and create a new variable:

```
$storageAccountKey = "<KEY1_STORAGE_ACCOUNT_KEY>"
```

8. Create additional variables:

```
$storageContainerName = "container1"  
$destinationVHDFileName = "disk1.vhd"  
$useAzCopy = 1  
$vmName = "winVM"
```

9. Stop the VM:

```
Stop-AzVM -ResourceGroupName $rg -Name  
$vmName
```

Take a Snapshot of the VM

1. Use the appropriate commands to take a snapshot of the VM.

2. Once the VM has stopped, grant access to the disk:

```
$sas = Grant-AzDiskAccess -  
ResourceGroupName $rg -DiskName $diskName  
-DurationInSecond $sasExpiryDuration -  
Access Read
```

3. Create an Azure Storage context:

```
$destinationContext = New-  
AzStorageContext -StorageAccountName  
$storageAccountName -StorageAccountKey  
$storageAccountKey
```

Copy the Snapshot to Container

1. Using AzCopy, send the snapshot to the `container1` within the storage account provisioned with this lab.
2. o Using AzCopy, send the snapshot to `container1`:

```
if($useAzCopy -eq 1)
{
    $containerSASURI = New-AzStorageContainerSASToken -Context
    $destinationContext -ExpiryTime(get-
    date).AddSeconds($sasExpiryDuration) -
    FullUri -Name $storageContainerName -
    Permission rw
    azcopy copy $sas.AccessSAS
    $containerSASURI

} else{

    Start-AzStorageBlobCopy -AbsoluteUri
    $sas.AccessSAS -DestContainer
    $storageContainerName -DestContext
    $destinationContext -DestBlob
    $destinationVHDFFileName
}
```

Create an image from a VM and deploy to scale set:

Create an Image from the VM

1. Create an image gallery (**NOTE**: you will need to add some characters to the end of the gallery name to make it unique):

```
az sig create --resource-group $RG --location westus --gallery-name imageGallery
```

2. Create an image definition:

```
az sig image-definition create \
--resource-group $RG \
--location westus \
--gallery-name imageGallery \
--gallery-image-definition imageDefinition \
--publisher acg \
--offer ubuntu \
--sku Ubuntu-1804 \
--os-type Linux \
--os-state specialized \
--features IsAcceleratedNetworkSupported=True
```

3. Create an image version:

```
az sig image-version create \
--resource-group $RG \
--location westus \
--gallery-name imageGallery \
--gallery-image-definition imageDefinition \
--gallery-image-version 1.0.0 \
--target-regions "westus=1" "eastus=1" \
--managed-image $IMAGE
```

Create a Virtual Machine Scale Set from an Image

1. In the Azure portal, scroll the listed resources and click the new image definition file.
2. In the left menu, click **Properties**.
3. Scroll down and copy the Resource ID to the clipboard.
4. In Cloud Shell, create a VM scale set, replacing `<RESOURCE_ID>` in the `image` variable with the name you just copied:

```
az vmss create \
--resource-group $RG \
--name myVmss \
--image "<RESOURCE_ID>" \
--specialized \
--generate-ssh-key \
--location westus
```

5. To confirm results in the Azure portal, scroll the listed resources and click **myVMss > Instances**. You should see two VMs running.

Ruta para la variable del id de la imagen:

```
cloud@Azure:~$ az vmss create \
> --resource-group $RG \
> --name myVmss \
> --image "/subscriptions/0f39574d-d756-48cf-b622-0e27a6943bd2/resourceGroups/421-dc15bce9-using-custo
m-images-for-a-virtual-mac/providers/Microsoft.Compute/galleries/imageGallery/images/imageDefinition"
\
```

1. Imagine que es administrador de varias máquinas virtuales de Azure. Recibe un mensaje de texto que indica algunos problemas en las máquinas virtuales. Está en la casa de un amigo y solo tiene disponible la tableta. Verdadero o falso: Puede acceder a la CLI de Azure con la tableta, aunque no puede instalar la CLI en ella. *

Verdadero

✓ Azure Cloud Shell está disponible en el explorador y se ejecuta con la CLI de Azure completa. Si prefiere PowerShell, Azure Cloud Shell también lo incluye.

Falso

2. Imagine que tiene un script que crea varias máquinas virtuales con imágenes diferentes. Cuando el script emite el comando para crear la primera máquina virtual, no quiere bloquear el script mientras se crea la máquina virtual, sino que quiere que pase inmediatamente al comando siguiente. ¿Cuál es la mejor forma de hacerlo? *

- Agregar el argumento '--async' al comando de creación.
 Usar la y comercial (&) para ejecutar el proceso en segundo plano.

Agregar el argumento '--no-wait' al comando de creación.

✓ La incorporación de '--no-wait' hace que se devuelva 'azure VM create' inmediatamente sin esperar a que la máquina virtual se cree realmente.

3. La mayoría de los comandos de Azure devuelven JSON de forma predeterminada. A veces, este conjunto de datos puede ser muy grande, lo que dificulta la lectura y el empleo del resultado de un comando como entrada para otro comando. ¿Qué puede usar con la CLI de Azure para filtrar los resultados a fin de obtener solo los datos que necesita? *

Puede usar el argumento '--query'.

✓ Todos los comandos de Azure admiten el argumento '--query', que permite seleccionar los datos útiles en cualquier respuesta de comando de Azure.

Puede usar el argumento '--filter'.

✗ La CLI de Azure no tiene ningún argumento '--filter'.

Puede canalizar los resultados a una utilidad de análisis de JSON y usar capacidades de filtrado allí.

1. When creating a Windows virtual machine in Azure, which port would you open using the INBOUND PORT RULES in order to allow remote-desktop access? *

- HTTPS
- SSH (22)
- RDP (3389)

 The Remote Desktop Protocol (RDP) uses port 3389 by default so this port is the standard port you would open if you wanted to use an RDP client to administer your Windows virtual machines.

2. Suppose you have an application running on a Windows virtual machine in Azure. What is the best-practice guidance on where the app should store data files? *

- OS disk (C:)
- Temporary disk (D:)
- Attached data disk

 Dedicated data disks are generally considered the best place to store application data files. They can be larger than OS disks and you can optimize them for the cost and performance characteristics appropriate for your data.

3. What is the final rule that is applied in every Network Security Group? *

- Allow All
- Deny All

 This is a safe choice. It will block all traffic that you don't specifically allow.

- You configure the final rule to your needs

1. True or false: Azure App service can automatically scale your web application to meet traffic demand. *

True

- ✓ Azure App service has built-in autoscale support and will increase or decrease the resources allocated to run your app as needed, depending on the demand.

False

2. Which of the following isn't a valid automated deployment source? *

GitHub

Azure DevOps

SharePoint

- ✓ Azure currently supports Azure DevOps, GitHub, Bitbucket, OneDrive, Dropbox, and external Git repositories.

Managing Virtual Machine Updates

MANAGING VIRTUAL MACHINE UPDATES

Describing Update Management

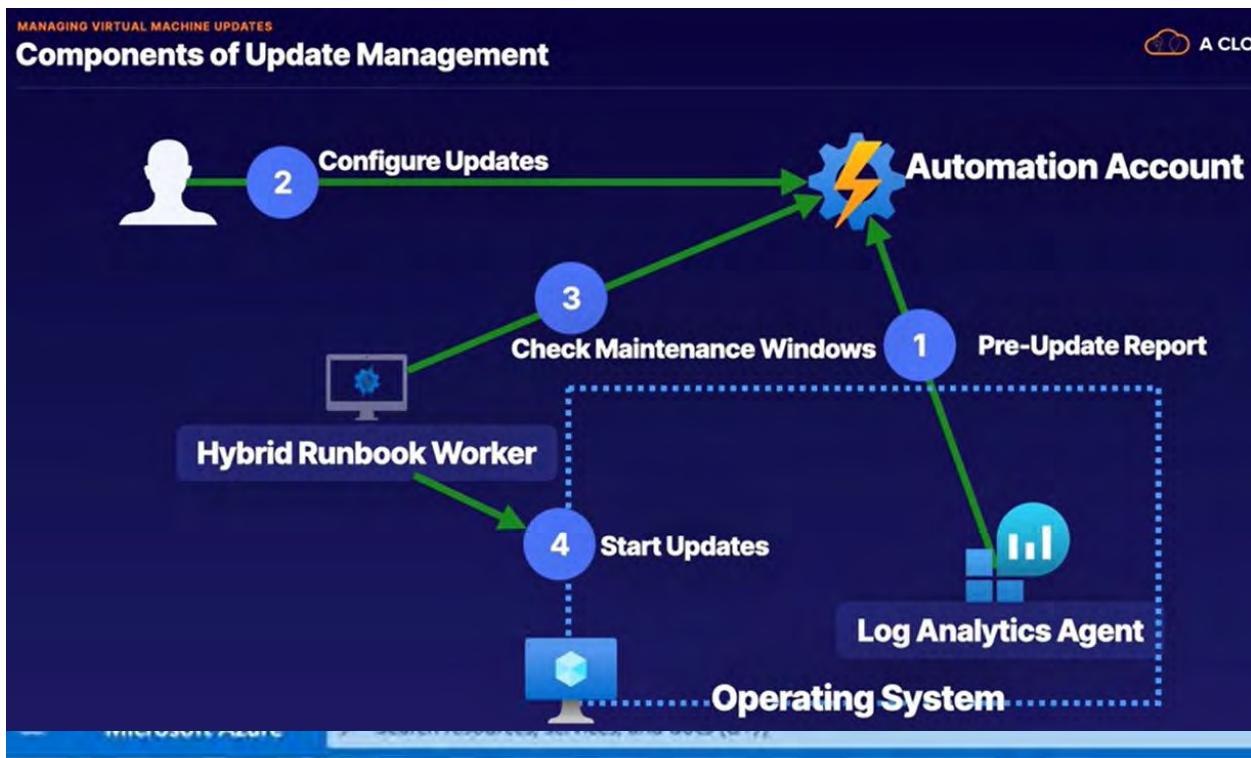
A CLOUD

Update Management



Manages system updates and patches for workloads both in the Azure cloud and on-premises.

- Supports Linux and Windows VMs
- Provides capabilities for:
 - Scheduling
 - Compliance scanning
 - Reporting



[Home](#) > [CreateVm-MicrosoftWindowsServer.WindowsServer-201-20210627143139](#) > [update-vm-01](#) >

Update Management (update-vm-01 - VM)

Update Management

Enable consistent control and compliance of this VM with Update Management.

This service is included with Azure virtual machines and Azure Arc machines. You only pay for logs stored in Log Analytics.

This service requires a Log Analytics workspace and an Automation account. You can use your existing workspace and account or let us configure the nearest workspace and account for use.

Log Analytics workspace location ⓘ

East US 2

Log Analytics workspace ⓘ

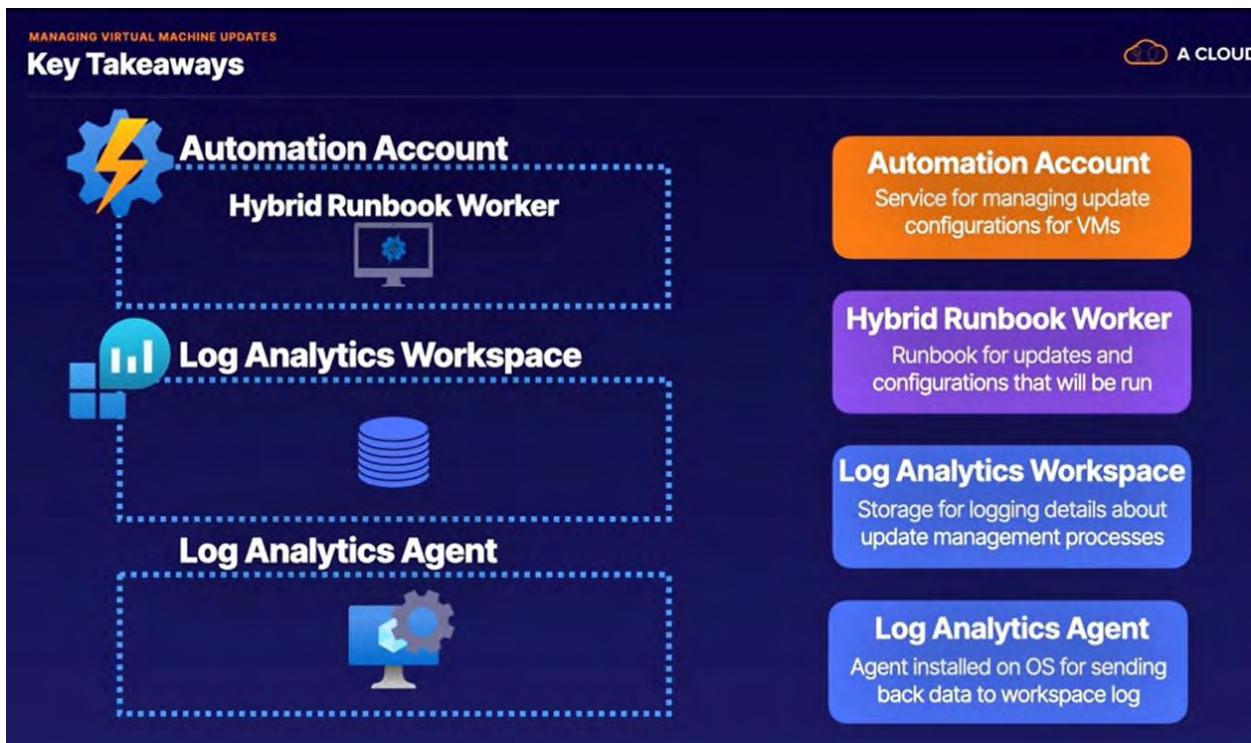
Create default workspace...

Automation account subscription ⓘ

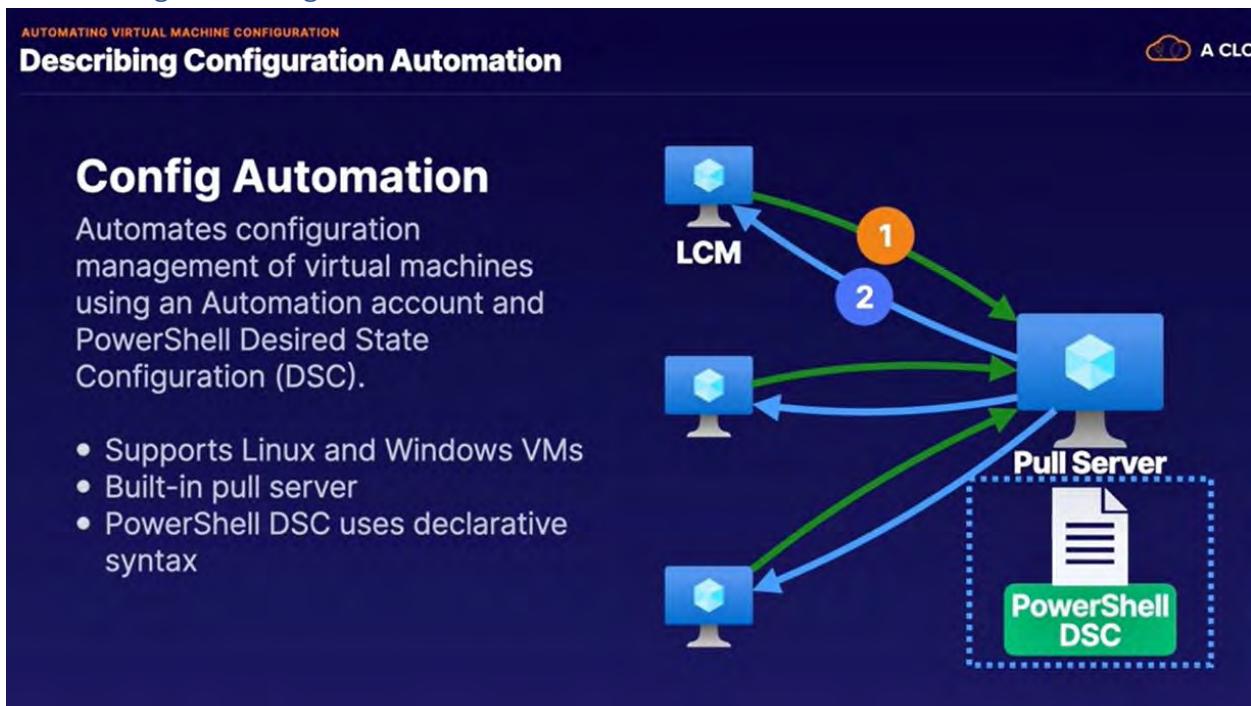
Cloud Chase MCT Subscription

Podemos manejar muchas maquinas y podemos agendar los updates del SO.

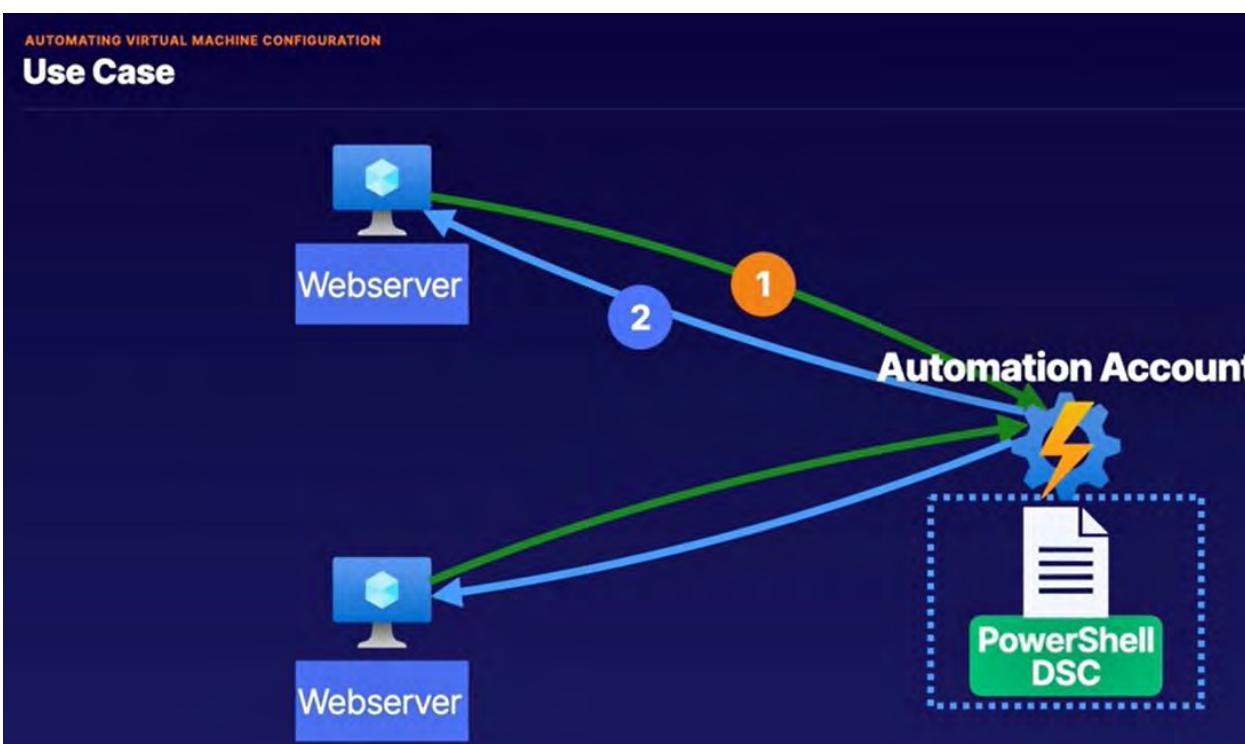
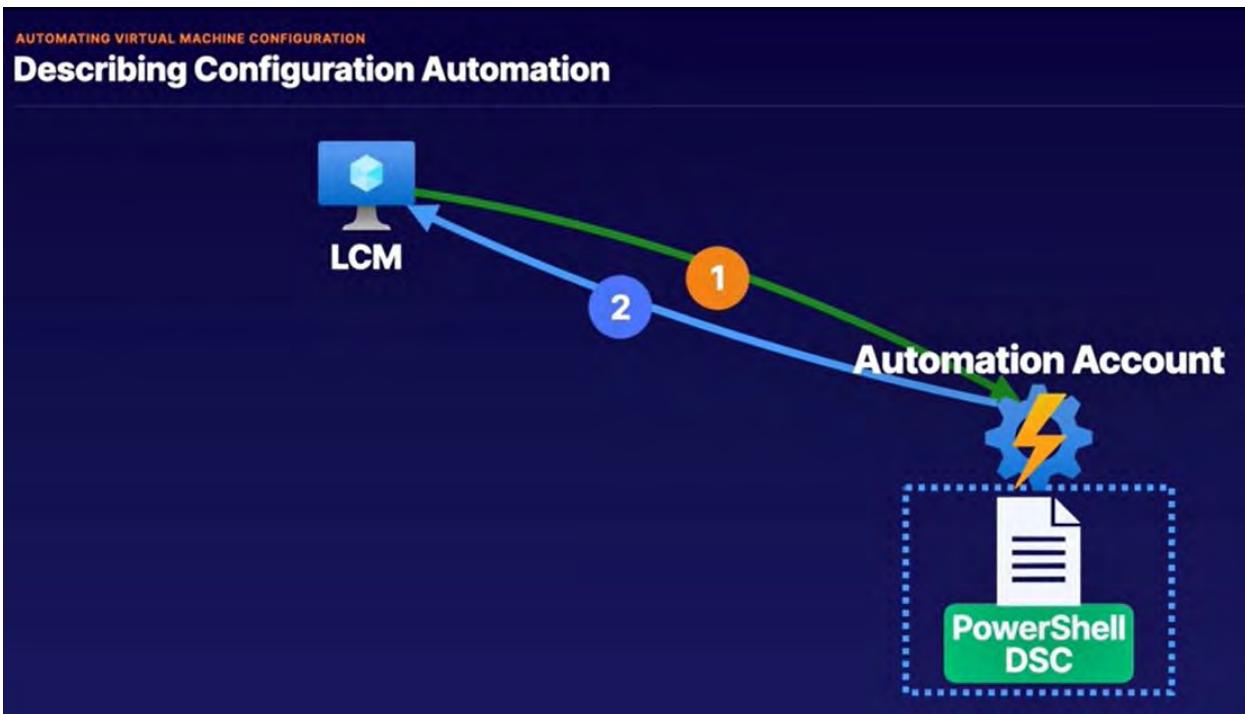
Instala un log agent en la compus para estar monitoreando el equipo.



Automating VM configuration



La VM checa el dsc en la automation account y ve tiene que hacer cambios o no:



Al añadir un dsc hay que compilarlo para ver que este correcto

Automation Account

Service for managing update configurations for VMs

PowerShell DSC

PowerShell scripts that declare desired state of VMs

Local Configuration Manager

Sends current config state to pull server for evaluation

Implement virtual machines extensions

100 XP

3 minutes

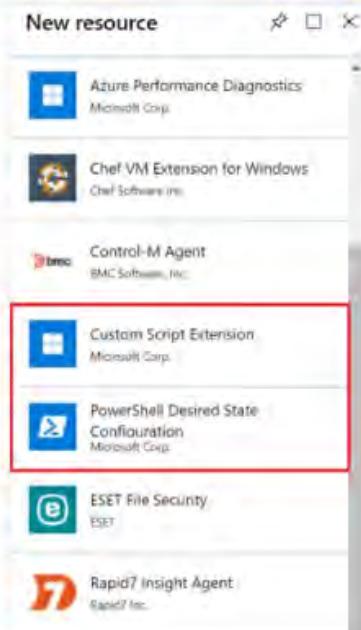
Creating and maintaining virtual machines can be burdensome. Many of the maintenance tasks are repetitive and time-consuming. Fortunately, there are several ways to automate the tasks of creating, maintaining, and removing virtual machines. One way is to use a virtual machine extension.

Azure virtual machine extensions are small applications that provide post-deployment configuration and automation tasks for Azure Virtual Machines. Consider a scenario where a virtual machine requires software installation or anti-virus protection, or when a machine needs to run a configuration script. You can use virtual machine extensions to complete these tasks. Extensions are all about managing your virtual machines.

Things to know about virtual machine extensions

Examine the following characteristics of virtual machine extensions.

- You can manage virtual machine extensions with the Azure CLI, PowerShell, Azure Resource Manager (ARM) templates, and the Azure portal.
- Virtual machine extensions can be bundled with a new virtual machine deployment or run against any existing system.
- There are different virtual machine extensions for Windows and Linux machines. You can choose from a large set of first and third-party virtual machine extensions.



Things to consider when using virtual machine extensions

Let's review some example scenarios for working with virtual machine extensions. Think about how can you implement virtual machines extensions to support your organization.

- Consider deployment. Virtual machine extension small applications can be a subset of a larger deployment for your virtual machines.
- Consider provisioning. You can use virtual machine extensions as configuration applications to assist with provisioning your virtual machines.
- Consider post-deployment. Virtual machine extensions can be run against any supported extension operated systems after deployment.

Implement Custom Script Extensions

100 XP

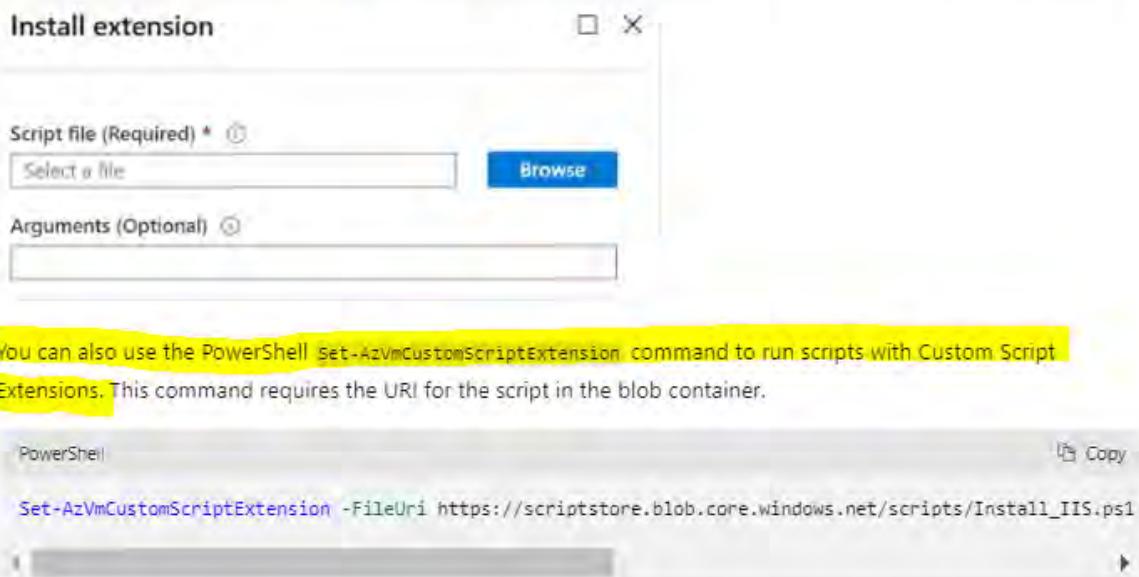
3 minutes

Custom Script Extensions can be used to automatically launch and execute virtual machine customization tasks after initial machine configuration. Your script extension can perform simple tasks such as stopping the virtual machine or installing a software component. Scripts can also be more complex and perform a series of tasks.

Things to know about Custom Script Extensions

Let's examine the details about working with Custom Script Extensions.

- You can install Custom Script Extensions from the Azure portal by accessing your virtual machine's Extensions page.
- After the Custom Script Extensions resource is created for your virtual machine, you provide a PowerShell script file with the commands to execute on the machine. You can also specify optional arguments, as required for your scenario. After your PowerShell file is uploaded, your script is executed immediately.
- Scripts can be downloaded from Azure Storage or GitHub, or provided to the Azure portal at extension run time.



Things to consider when using Custom Script Extensions

Review the following considerations regarding using Custom Script Extensions with virtual machines. Take a moment to assess how Custom Script Extensions can benefit your virtual machine configuration, deployment, and management tasks.

- Consider tasks that might time out. Keep in mind that Custom Script Extensions only have 90 minutes to execute. If your deployment takes longer than 90 minutes, your task is marked as a *timeout*. Be sure to consider the time-out period when you design your scripts. Your virtual machine must be running to be able to perform the designated tasks.
- Consider dependencies. Identify dependencies in your virtual machine task configuration. If your Custom Script Extension requires networking or storage access, make sure the content is available.
- Consider failure events. Plan for any errors that might occur when running your script. Identify scenarios where you might run out of disk space, or areas that have security and access restrictions. Establish a strategy for how your script responds to errors.
- Consider sensitive data. Your Custom Script Extension might need sensitive information such as credentials, storage account names, and storage account access keys. Think about how you to protect or encrypt your sensitive information.

Things to know about creating your Desired State Configuration

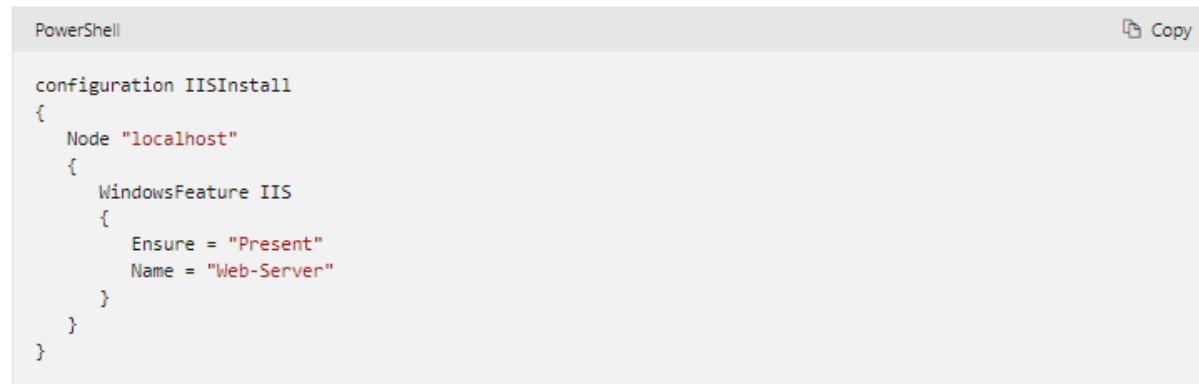
Review the following details about how to create a Desired State Configuration for your virtual machines.

- You can use Desired State Configuration when Custom Script Extensions don't satisfy the application requirements for your virtual machine.
- Desired State Configuration centers around [creating specific configurations](#) by using [scripts](#).
- A configuration is an [easy-to-read script](#) that describes an environment made up of computers (nodes) with specific characteristics. These characteristics can be as simple as ensuring a specific Windows feature is enabled or as complex as deploying SharePoint.
- The configuration script consists of a configuration block, node block, and one or more resource blocks.
 - The configuration block is the outermost script block. You define the block with the [Configuration](#) keyword and providing a name.
 - Node blocks define the computers or virtual machines that you're configuring. You define a node with the [Node](#) keyword and providing a name for the resource.
 - Resource blocks configure the resource (computers or virtual machines) properties. You provide the name of the Windows Role or Feature that you want to ensure is added or removed. The [Ensure](#) keyword is used to indicate if the Role or Feature is added.
- Desired State Configuration provides a set of Windows PowerShell language extensions, Windows PowerShell cmdlets, and resources. You can use these features to declaratively specify how you want your software environment to be configured.
- The Windows PowerShell Desired State Configuration comes with a set of built-in configuration resources, such as [File Resource](#), [Log Resource](#), and [User Resource](#).

Things to consider when using Desired State Configuration

Let's look at an example implementation for a Desired State Configuration. The following PowerShell script installs IIS on the localhost and ensures the web server is present. The configuration is saved as a PS1 file.

- The configuration block is named `IISInstall`.
- There's one node block that targets a computer resource named `localhost`.
- There's one resource block that specifies the Web-Server Windows Feature for IIS. The `Ensure` value indicates the Windows Feature is Present.



A screenshot of a PowerShell window titled "PowerShell". The window contains a single line of PowerShell code:

```
configuration IISInstall
```

The code defines a configuration block named `IISInstall`. It contains a node block for the computer `"localhost"`. Inside the node block, there is a resource block for the `WindowsFeature` named `IIS`. The `Ensure` parameter is set to `"Present"`, and the `Name` parameter is set to `"Web-Server"`. The entire configuration is enclosed in curly braces.

1. Which of the following options is a small application that provides post-deployment configuration and automation tasks for Azure Virtual Machines? *

Automation State Configuration

Desired State Configuration

✗ Incorrect. Desired State Configuration helps with deploying and managing configuration data for software services.

Virtual machine extensions

✓ Correct. Virtual machine extensions are small applications that automate the tasks of creating, maintaining, and removing virtual machines.

2. How soon do Custom Script Extensions time out? *

30 minutes

90 minutes

✓ Correct. Custom Script Extensions time out after 90 minutes. Always consider the time-out period when planning the scope of your script.

120 minutes

3. What option can the infrastructure team use for their IIS configuration instead of Custom Script Extensions? *

Desired State Configuration

✓ Correct. Desired State Configuration is a good choice for installing virtual machine features.

Virtual machine extension

1. What is Azure Automation State Configuration? *

- A declarative management platform to configure, deploy, and control systems.
- X PowerShell DSC is a declarative management platform to configure, deploy, and control systems.**
- A service used to write, manage, and compile PowerShell Desired State Configuration (DSC) configurations, import DSC resources, and assign configurations to target nodes.
- ✓ Azure Automation State Configuration enables you to ensure that all virtual machines in a collection are in the same consistent state.**
- A service that manages the state configuration on each destination, or node.

2. A PowerShell DSC script _____.*

- Contains the steps required to configure a virtual machine to get it into a specified state.**
- X A PowerShell DSC script is declarative. It describes the desired state but doesn't list the steps necessary to achieve that state.**
- Is idempotent.
- Describes the desired state.
- ✓ A PowerShell DSC script is declarative. It describes the desired state but doesn't include the steps necessary to achieve that state.**

3. Why should you use pull mode instead of push mode for DSC? *

- Pull mode is best for complex environments that need redundancy and scale.
- ✓ The local configuration manager (LCM) on each node automatically polls the pull server at regular intervals to get the latest configuration details. In push mode, an administrator manually sends the configurations toward the nodes.**
- Pull mode is easy to set up and doesn't need its own dedicated infrastructure.
- Pull mode uses the local configuration manager (LCM) to make sure that the state on each node matches the state specified by the configuration.**
- X Both pull mode and push mode use the LCM. The LCM is responsible for updating the configuration to match the desired state on a node.**

Using Azure Bastion

USING AZURE BASTION

What is Azure Bastion?

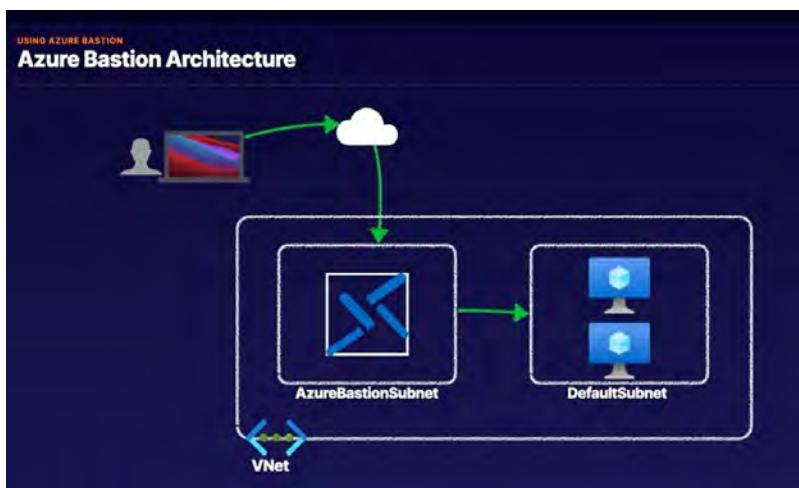


Facts

What is Azure Bastion?	Facts
Fully-managed PaaS	RDP/SSH connectivity over SSL/TLS
RDP/SSH connectivity	Deployed per virtual network
No public IPs exposed	Connectivity to all VMs in VNet
	HTML5 browser supported
	No public IPs
	Only supports IPv4

What is Azure Bastion?

- Fully-managed PaaS
- RDP/SSH connectivity
- No public IPs exposed



Crea una conexión al server por medio del bastion que se crea y es una conexión privada

USING AZURE BASTION

Key Takeaways



Private Traffic
Traffic from Bastion to target VM stays within VNets. (Peered VNets included.)

Concurrent Connections
Total maximum connections is 25 with RDP and 50 with SSH traffic.

Hardened Bastion
NSGs are not needed because Bastion is hardened internally.

Audit Logs
Enable diagnostics for auditing Bastion connections.

Service Integration
Bastion natively integrates with Azure Firewall.

Required Role
Reader role permissions are required on the Bastion, VM, and NIC in order to use Bastion.

Azure Load Balancers

INTRODUCING AZURE LOAD BALANCER

Describing Azure Load Balancer

A Cloud Guru

Azure Load Balancer (LB)

Azure Load Balancer is a networking solution for distributing traffic between backend compute.

- Layer 4 load balancing (TCP/UDP)
- High availability
- Backend resources must be redundant

```
graph LR; Internet((Internet)) --> PIP[PIP]; PIP --> VNet[VNet]; VNet --> AzureLB[Azure LB]; AzureLB --> VM1[VM]; AzureLB --> VM2[VM]; AzureLB --> VM3[VM]
```

INTRODUCING AZURE LOAD BALANCER

Components of an Azure Load Balancer

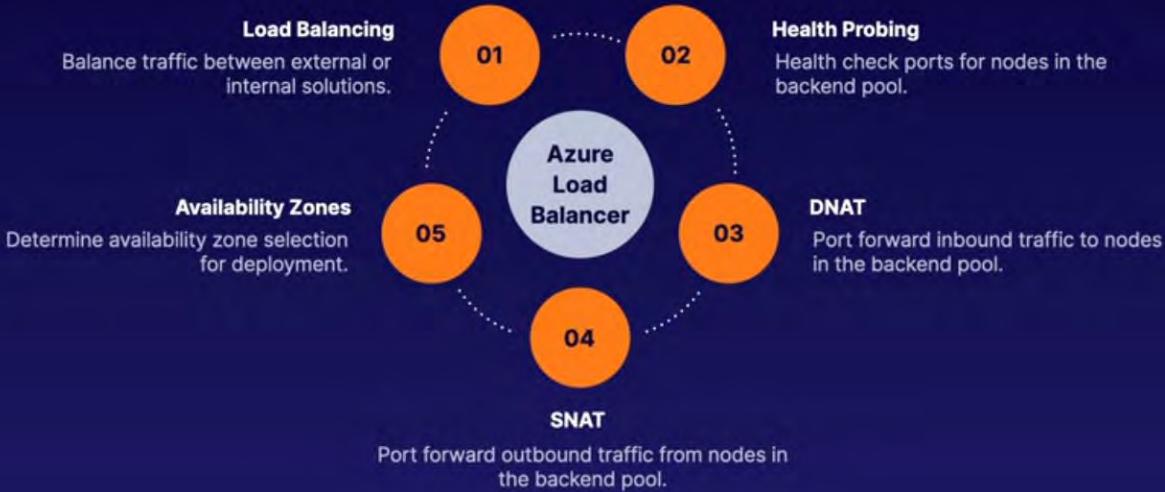
A Cloud Guru

10.0.0.0	Frontend IP Private or public endpoint for accessing the load balancing solution.
	Backend Pool Compute solution underlying the load balancer.
	Health Probe Probe that periodically checks the health of the backend pool to determine available nodes.
	Rules Load balancing or NAT rules configured for allowing inbound/outbound access.

```
graph LR; PIP[PIP] --> AzureLB[Azure LB]; AzureLB --> VM1[VM]; AzureLB --> VM2[VM]; Probe((Health Probe)) --- AzureLB
```

Key Takeaways

Next lesson
Create a Standard Load Balancer
with Azure CLI



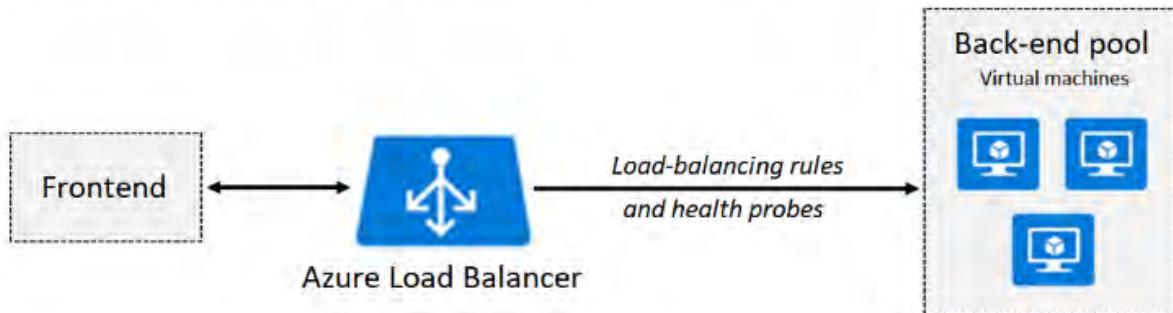
Determine Azure Load Balancer uses

✓ 100 XP

2 minutes

Azure Load Balancer delivers high availability and network performance to your applications. Administrators use load balancing to efficiently distribute incoming network traffic across back-end servers and resources. A load balancer is implemented by using load-balancing rules and health probes.

The following diagram shows how Azure Load Balancer works. The frontend exchanges information with a load balancer. The load balancer uses rules and health probes to communicate with the backend.



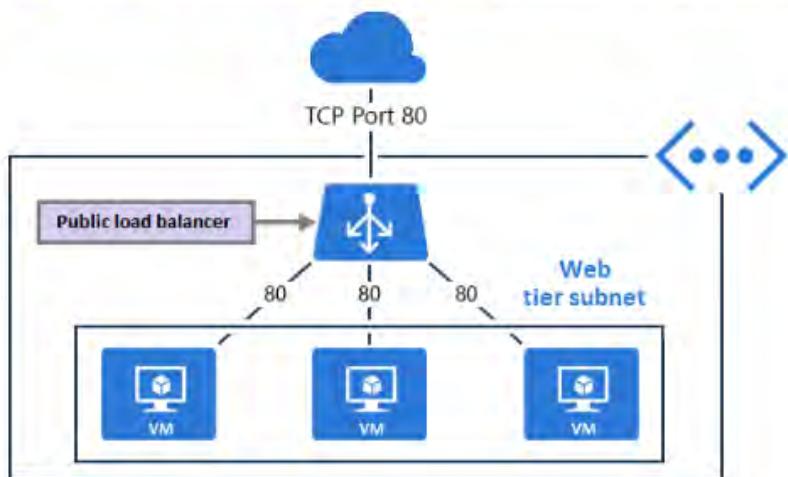
Things to know about Azure Load Balancer

Let's take a closer look at how Azure Load Balancer operates.

- Azure Load Balancer can be used for inbound and outbound scenarios.
- You can implement a public or internal load balancer, or use both types in a combination configuration.
- To implement a load balancer, you configure four components:
 - Front-end IP configuration
 - Back-end pools
 - Health probes
 - Load-balancing rules
- The front-end configuration specifies the public IP or internal IP that your load balancer responds to.
- The back-end pools are your services and resources, including Azure Virtual Machines or instances in Azure Virtual Machine Scale Sets.
- Load-balancing rules determine how traffic is distributed to back-end resources.
- Health probes ensure the resources in the backend are healthy.
- Load Balancer scales up to millions of TCP and UDP application flows.

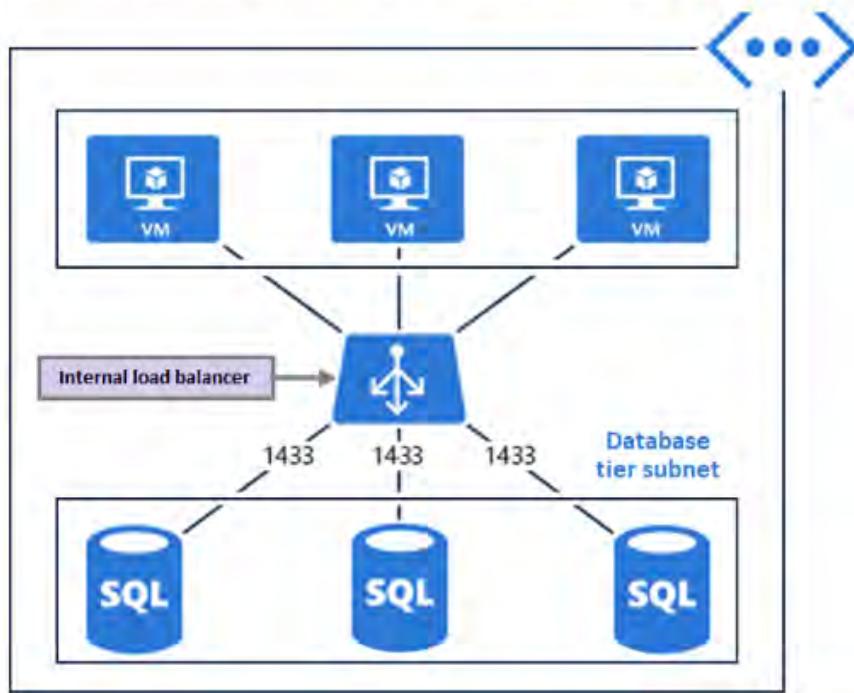
Business scenario

Consider a scenario where internet traffic attempts to reach virtual machines in a web tier subnet that implements a public load balancer. Internet clients send webpage requests to the public IP address of a web app on TCP port 80. Azure Load Balancer intercepts the traffic and distributes the requests across the virtual machines in the load-balanced set according to the defined load-balancing rules. The following illustration highlights this scenario:



Business scenario

Suppose you have an Azure SQL Database tier subnet with several virtual machines, and you implement an internal load balancer. Database requests need to be distributed to the backend. The internal load balancer receives the database requests and uses the load-balancing rules to determine how to distribute the requests to the back-end SQL servers. The SQL servers respond on port 1433. The following illustration highlights this scenario:



Things to consider when using an internal load balancer

You can implement an internal load balancer to achieve several types of load balancing.

- Within virtual network: Establish load balancing from your virtual machines in the virtual network to a set of virtual machines that reside within the same virtual network.
- For cross-premises virtual network: Apply load balancing from your on-premises computers to a set of virtual machines that reside within the same virtual network.
- For multi-tier applications: Implement load balancing for your internet-facing multi-tier applications when the back-end tiers aren't internet-facing. The back-end tiers require traffic load-balancing from the internet-facing tier.
- For line-of-business applications: Add load balancing for your line-of-business applications hosted in Azure without having to add other load balancer hardware or software. This scenario includes on-premises servers that are in the set of computers whose traffic is load-balanced.
- With public load balancer: Configure a public load balancer in front of your internal load balancer to create a multi-tier application.

Determine load balancer SKUs

✓ 100 XP

2 minutes

When you create an Azure load balancer in the Azure portal, you select the type of load balancer to create (internal or public) and the SKU. Azure Load Balancer supports three SKU options: Basic, Standard, and Gateway. Each SKU provides different features, scenario scaling, and pricing.

Things to know about Azure Load Balancer SKUs

Let's review some points to consider when choosing the SKU type for your load balancer.

- Standard Load Balancer is the newest product. It's essentially a superset of Basic Load Balancer.
- The Standard SKU offers an expanded and more granular feature set than the Basic SKU.
- The Basic SKU can be upgraded to the Standard SKU. But, new designs and architectures should use the Standard SKU.
- The Gateway SKU supports high performance and high availability scenarios with third-party network virtual appliances (NVAs).

Compare Basic and Standard SKU features

The following table provides a brief comparison of how features are implemented in the Standard and Basic SKUs.

Feature	Basic SKU	Standard SKU
Health probes	HTTP, TCP	HTTPS, HTTP, TCP
Availability zones	Not available	Zone-redundant and zonal frontends for inbound and outbound traffic
Multiple frontends	Inbound only	Inbound and outbound
Security	- Open by default - (Optional) Control through network security groups (NSGs)	- Closed to inbound flows unless allowed by an NSG - Internal traffic from the virtual network to the internal load balancer is allowed

Things to know about back-end pools

The SKU type that you select determines which endpoint configurations are supported for the pool along with the number of pool instances allowed.

- The Basic SKU allows up to 300 pools, and the Standard SKU allows up to 1,000 pools.
- When you configure the back-end pools, you can connect to availability sets, virtual machines, or Azure Virtual Machine Scale Sets.
- For the Basic SKU, you can select virtual machines in a single availability set or virtual machines in an instance of Azure Virtual Machine Scale Sets.
- For the Standard SKU, you can select virtual machines or Virtual Machine Scale Sets in a single virtual network. Your configuration can include a combination of virtual machines, availability sets, and Virtual Machine Scale Sets.

Create health probes

✓ 100 XP

2 minutes

A health probe allows your load balancer to monitor the status of your application. The probe dynamically adds or removes virtual machines from your load balancer rotation based on the machine response to health checks. When a probe fails to respond, the load balancer stops sending new connections to the unhealthy instance.

The following image shows how to create a health probe in the Azure portal. A custom HTTP health probe is configured to run on TCP port 80. The probe is defined to check the health of the virtual machine instances at 5-second intervals.

Things to know about health probes

There are two main ways to configure a custom health probe: HTTP and TCP.

- In an HTTP probe, the load balancer probes your back-end pool endpoints every 15 seconds. A virtual machine instance is considered *healthy* if it responds with an HTTP 200 message within the specified timeout period (default is 31 seconds). If any status other than HTTP 200 is returned, the instance is considered *unhealthy*, and the probe fails.
- A TCP probe relies on establishing a successful TCP session to a defined probe port. If the specified listener on the virtual machine exists, the probe succeeds. If the connection is refused, the probe fails.
- To configure a probe, you specify values for the following settings:
 - Port: Back-end port
 - URI: URI for requesting the health status from the backend
 - Interval: Amount of time between probe attempts (default is 15 seconds)
 - Unhealthy threshold: Number of failures that must occur for the instance to be considered unhealthy
- A Guest agent probe is a third option that uses the guest agent inside the virtual machine. This option isn't recommended when an HTTP or TCP custom probe configuration is possible.

Things to know about load-balancing rules

Let's take a closer look at how to configure load-balancing rules for your back-end pools.

- To configure a load-balancing rule, you need to have a frontend, backend, and health probe for your load balancer.
- To define a rule in the Azure portal, you configure several settings:
 - IP version (IPv4 or IPv6)
 - Front-end IP address, *Port, and Protocol (TCP or UDP)
 - Back-end pool and Back-end port
 - Health probe
 - Session persistence
- By default, Azure Load Balancer distributes network traffic equally among multiple virtual machines.

Azure Load Balancer uses a five-tuple hash to map traffic to available servers. The tuple consists of the source IP address, source port, destination IP address, destination port, and protocol type. The load balancer provides stickiness only within a transport session.

- Session persistence specifies how to handle traffic from a client. By default, successive requests from a client are handled by any virtual machine in your pool.

You can modify the session persistence behavior as follows:

- None (default): Any virtual machine can handle the request.
- Client IP: Successive requests from the same client IP address are handled by the same virtual machine.
- Client IP and protocol: Successive requests from the same client IP address and protocol combination are handled by the same virtual machine.

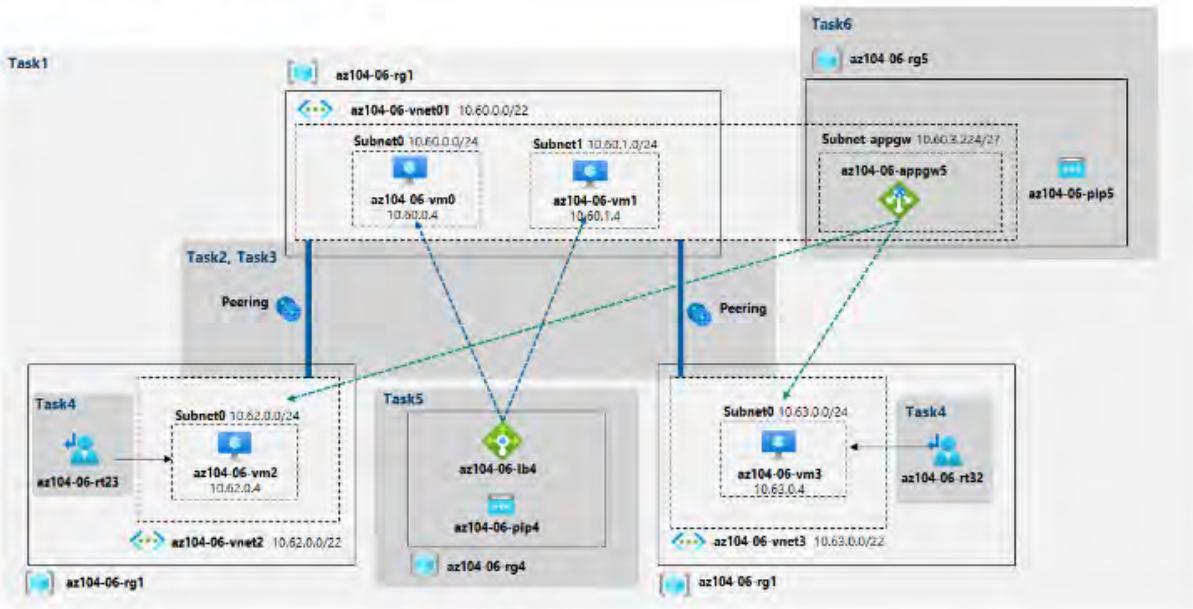
① Note

Maintaining session persistence information is important for applications that implement a shopping cart. Can you think of other applications that might benefit from session persistence?

- Load-balancing rules can be used in combination with NAT rules.

Consider a scenario where you use NAT from a load balancer's public address to TCP port 3389 on a specific virtual machine. By combining your NAT rule with load-balancing rules, you can enable remote desktop access from outside of Azure.

Architecture diagram



Answer the following questions

Choose the best response for each of the following questions. Then select Check your answers.

1. What's the default distribution type for traffic through a load balancer? *

- Source IP affinity
- Three-tuple hash
- Five-tuple hash

✓ Correct. The load balancer uses a five-tuple (source IP, source port, destination IP, destination port, and protocol type) hash to map traffic to available servers.

2. Which configuration is required for an internal load balancer? *

- Virtual machines must be in the same virtual network.
- Virtual machines must be publicly accessible.
- Virtual machines must be in an availability set.

1. What is the default distribution type for traffic through a load balancer? *

- Source IP affinity
 - Five-tuple hash
- ✓ Five-tuple hash is the default.

- Three-tuple hash

2. What is the main advantage of an availability set? *

- It allows virtual machines to be available across datacenter failures.
✗ Availability zones, not availability sets, provide availability across datacenter failures.
- It allows virtual machines to be available across physical server failures.
✓ Availability sets allow virtual machines to remain available when a physical server fails.
- It allows virtual machines to be grouped into logical categories.

1. Which configuration is required to configure an internal load balancer? *

- Virtual machines must be in the same virtual network.
✓ The virtual machines that you use a load balancer to distribute a load to must be in the same virtual network.
- Virtual machines must be publicly accessible.
- Virtual machines must be in an availability set.

2. Which one of the following statements about external load balancers is correct? *

- They have a private, front-facing IP address.
✗ External load balancers have public IP addresses.
- They don't have a listener IP address.
- They have a public IP address.
✓ External load balancers have public IP addresses.

Using Application Gateway

USING APPLICATION GATEWAY

Describing Azure Application Gateway

A CLOUD GURU

Azure Application Gateway (App GW)

Azure Application Gateway is a networking service for load balancing between backend compute.

- Layer 7 load balancing (HTTP/HTTPS)
- URL path-based routing
- Backend resources must be redundant

USING APPLICATION GATEWAY

Components of an Application Gateway

A CLOUD GURU

	Frontend IP 10.0.0.0 Private or public endpoint for accessing the load balancing solution.
	Backend Pool Compute solution underlying the load balancer.
	Listener Port, protocol, and certificate configurations.
	Rules Load balancing rules, HTTP settings, and health probe.

La subnet que debemos crear para el app Gateway debe ser de /27

Media la URL path el app Gateway sabe para que server debe ir dependiendo de como lo configuremos



Implement Azure Application Gateway

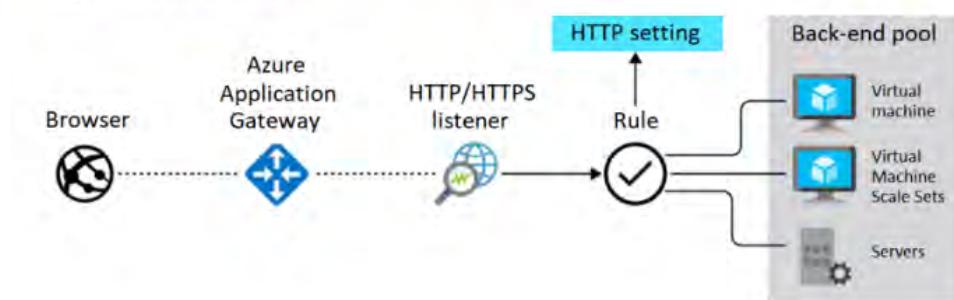
✓ 100 XP

3 minutes

Administrators use Azure Application Gateway to manage requests from client applications to their web apps. An application gateway listens for incoming traffic to web apps and checks for messages sent via protocols like HTTP. Gateway rules direct the traffic to resources in a back-end pool.

Business scenario

Consider a scenario where internet client applications request access to resources in a load-balanced back-end pool. The requests can be managed by implementing Azure Application Gateway to listen for HTTP(S) messages. Messages can be handled by load-balancing rules to direct client request traffic to the appropriate resources in the pool. The following diagram illustrates this scenario:



Things to know about Azure Application Gateway

Let's examine some of the benefits of using Azure Application Gateway to manage internet traffic to your web applications.

Benefit	Description
Application layer routing	Use application layer routing to direct traffic to a back-end pool of web servers based on the URL of a request. The back-end pool can include Azure virtual machines, Azure Virtual Machine Scale Sets, Azure App Service, and even on-premises servers.
Round-robin load balancing	Employ round-robin load balancing to distribute incoming traffic across multiple servers. Send load-balance requests to the servers in each back-end pool. Client requests are forwarded in a cycle through a group of servers to create an effective balance for the server load.
Session stickiness	Apply session stickiness to your application gateway to ensure client requests in the same session are routed to the same back-end server.
Supported protocols	Build an application gateway to support the HTTP, HTTPS, HTTP/2, or WebSocket protocols.
Firewall protection	Implement a web application firewall to protect against web application vulnerabilities.
Encryption	Support end-to-end request encryption for your web applications.
Load autoscaling	Dynamically adjust capacity as your web traffic load changes.

Things to know about traffic routing

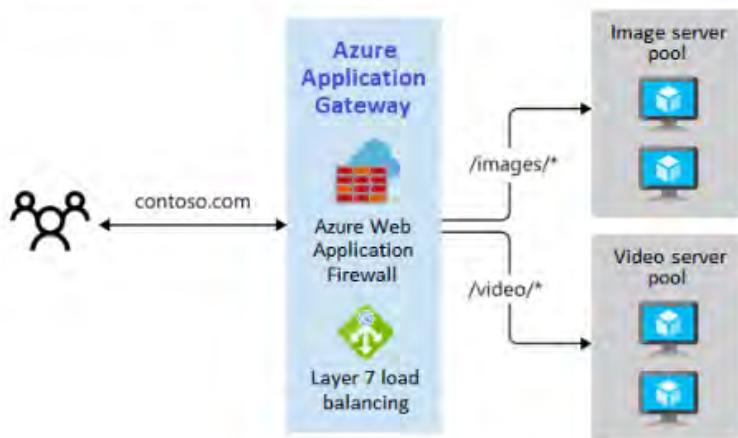
Let's take a closer look at your routing options for Azure Application Gateway.

- Azure Application Gateway offers two primary methods for routing traffic:
 - Path-based routing sends requests with different URL paths to different pools of back-end servers.
 - Multi-site routing configures more than one web application on the same application gateway instance.
- You can configure your application gateway to redirect traffic. Application Gateway can redirect traffic received at one listener to another listener, or to an external site. This approach is commonly used by web apps to automatically redirect HTTP requests to communicate via HTTPS. The redirection ensures all communication between your web app and clients occurs over an encrypted path.
- You can implement Application Gateway to rewrite HTTP headers. HTTP headers allow the client and server to pass parameter information with the request or the response. In this scenario, you can translate URLs or query string parameters, and modify request and response headers. Add conditions to ensure URLs or headers are rewritten only for certain conditions.
- Application Gateway allows you to create custom error pages instead of displaying default error pages. You can use your own branding and layout by using a custom error page.

Path-based routing

You can implement path-based routing to direct requests for specific URL paths to the appropriate back-end pool.

Consider a scenario where your web app receives requests for videos or images. You can use path-based routing to direct requests for the `/video/*` path to a back-end pool of servers that are optimized to handle video streaming. Image requests for the `/images/*` path can be directed to a pool of servers that handle image retrieval. The following illustration demonstrates this routing method:

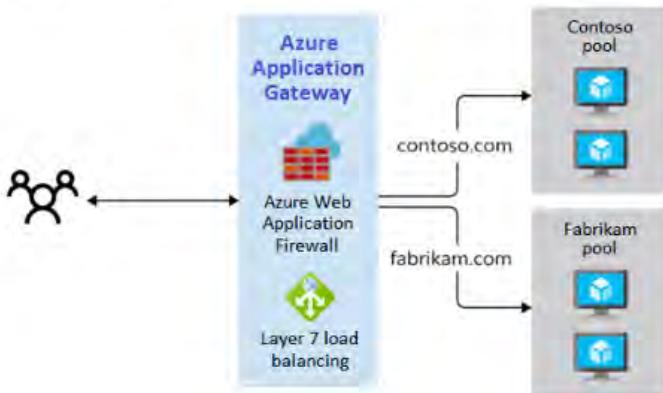


Multi-site routing

When you need to support multiple web apps on the same application gateway instance, multi-site routing is the best option. Multi-site configurations are useful for supporting multi-tenant applications, where each tenant has its own set of virtual machines or other resources hosting a web application.

In this configuration, you register multiple DNS names (CNAMEs) for the IP address of your application gateway and specify the name of each site. Application Gateway uses separate listeners to wait for requests for each site. Each listener passes the request to a different rule, which can route the requests to servers in a different back-end pool.

Consider a scenario where you need to support traffic to two sites on the same gateway. You can direct all requests for the `http://contoso.com` site to servers in one back-end pool, and requests for the `http://fabrikam.com` site to another back-end pool. The following illustration demonstrates this routing method.

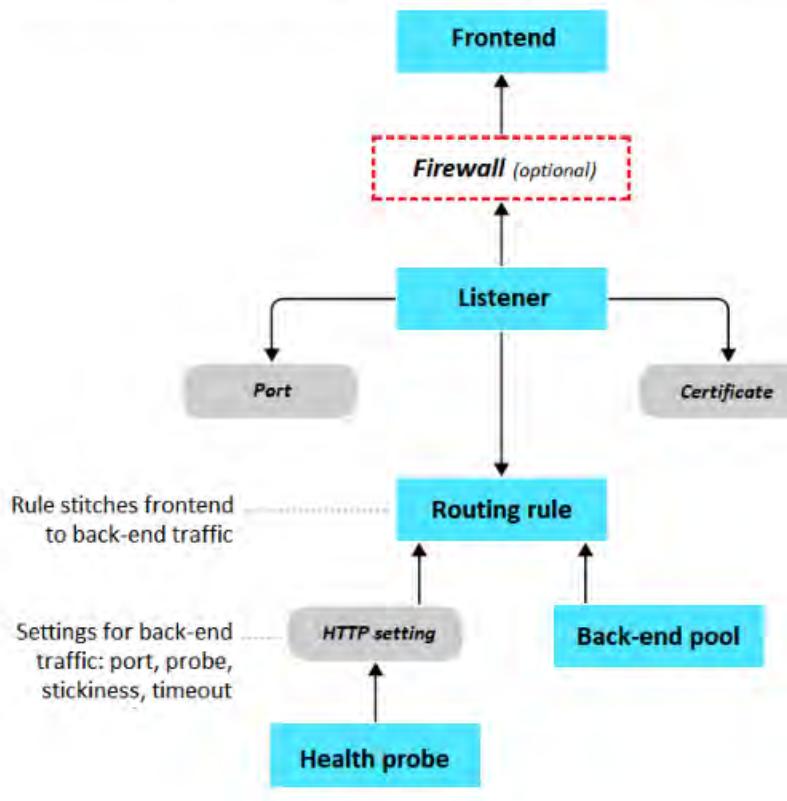


Things to know about Application Gateway components

Let's explore how the components of an application gateway work together.

- The front-end IP address receives the client requests.
- An optional firewall checks incoming traffic for common threats before the requests reach the listeners.
- One or more listeners receive the traffic and route the requests to the back-end pool.
- Routing rules define how to analyze the request to direct the request to the appropriate back-end pool.
- A back-end pool contains web servers for resources like virtual machines or Virtual Machine Scale Sets. Each pool has a load balancer to distribute the workload across the resources.
- Health probes determine which back-end pool servers are available for load-balancing.

The following flowchart demonstrates how the Application Gateway components work together to direct traffic requests between the frontend and back-end pools in your configuration.



Front-end IP address

Client requests are received through your front-end IP address. Your application gateway can have a public or private IP address, or both. You can have only one public IP address and only one private IP address.

Listeners

Listeners accept traffic arriving on a specified combination of protocol, port, host, and IP address. Each listener routes requests to a back-end pool of servers according to your routing rules. A listener can be *Basic* or *Multi-site*. A Basic listener only routes a request based on the path in the URL. A Multi-site listener can also route requests by using the hostname element of the URL. Listeners also handle TLS/SSL certificates for securing your application between the user and Application Gateway.

Routing rules

A routing rule binds your listeners to the back-end pools. A rule specifies how to interpret the hostname and path elements in the URL of a request, and then direct the request to the appropriate back-end pool. A routing rule also has an associated set of HTTP settings. These HTTP settings indicate whether (and how) traffic is encrypted between Application Gateway and the back-end servers. Other configuration information includes protocol, session stickiness, connection draining, request timeout period, and health probes.

Back-end pools

A back-end pool references a collection of web servers. You provide the IP address of each web server and the port on which it listens for requests when configuring the pool. Each pool can specify a fixed set of virtual machines, Virtual Machine Scale Sets, an app hosted by Azure App Services, or a collection of on-premises servers. Each back-end pool has an associated load balancer that distributes work across the pool.

Health probes

Health probes determine which servers in your back-end pool are available for load-balancing. Application Gateway uses a health probe to send a request to a server. When the server returns an HTTP response with a status code between 200 and 399, the server is considered healthy. If you don't configure a health probe, Application Gateway creates a default probe that waits for 30 seconds before identifying a server as unavailable (unhealthy).

Firewall (optional)

You can enable Azure Web Application Firewall for Azure Application Gateway to handle incoming requests before they reach your listener. The firewall checks each request for threats based on the Open Web Application Security Project (OWASP). Common threats include SQL-injection, cross-site scripting, command injection, HTTP request smuggling and response splitting, and remote file inclusion. Other threats can come from bots, crawlers, scanners, and HTTP protocol violations and anomalies.

OWASP defines a set of generic rules for detecting attacks. These rules are referred to as the Core Rule Set (CRS). The rule sets are under continuous review as attacks evolve in sophistication. Azure Web Application Firewall supports two rule sets: CRS 2.2.9 and CRS 3.0. CRS 3.0 is the default and more recent of these rule sets. If necessary, you can opt to select only specific rules in a rule set to target certain threats. Additionally, you can customize the firewall to specify which elements in a request to examine, and limit the size of messages to prevent massive uploads from overwhelming your servers.

Answer the following questions

Choose the best response for each of the following questions. Then select Check your answers.

1. What criteria does Azure Application Gateway use to route requests to a web server? *

The region where the servers hosting the web application are located.

The hostname, port, and path in the URL of the request.

✓ Correct. Application Gateway uses the hostname, port, and URL path.

The user's authentication information.

2. Which load-balancing strategy does Azure Application Gateway implement? *

Requests are distributed to the server in the back-end pool with the lightest load.

Each server in the back-end pool is polled in turn, and the request is sent to the first server that responds.

Requests are distributed to each available server in a back-end pool in turn via a round-robin technique.

✓ Correct. Application Gateway distributes requests across multiple servers by using a round-robin technique.

3. How can the concerns about security threats be addressed? *

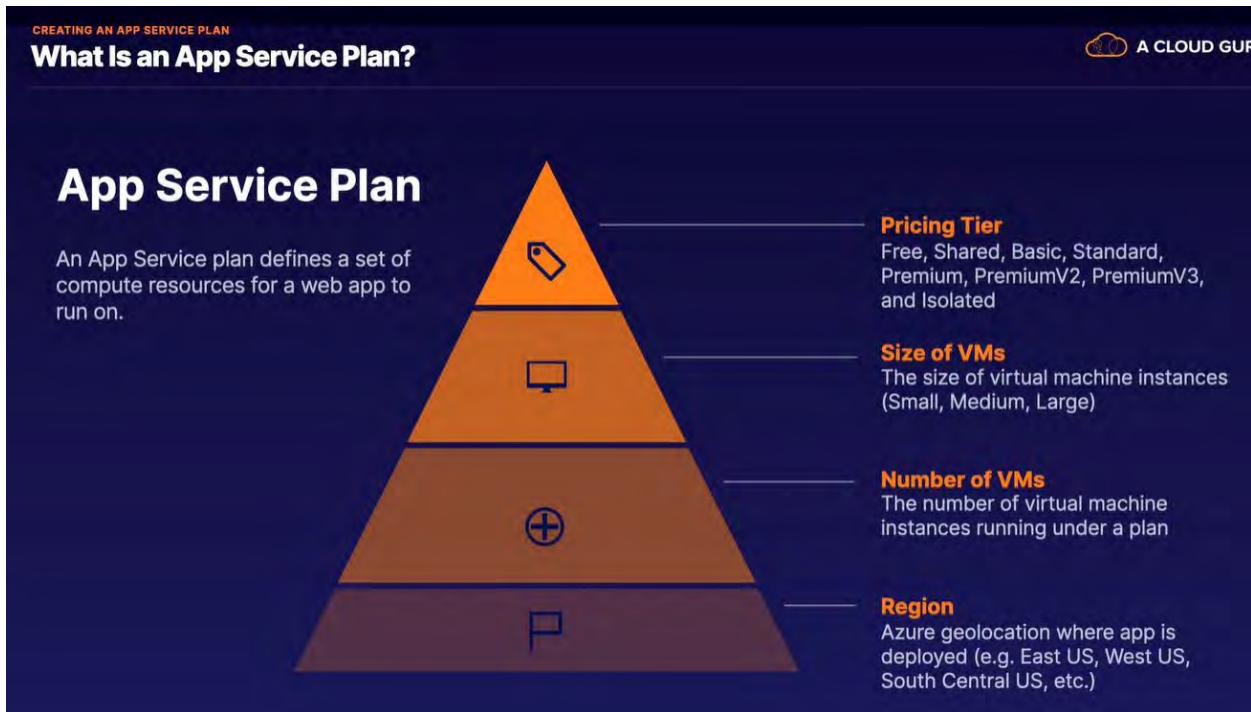
Install Azure Web Application Firewall.

✓ Correct. Azure Web Application Firewall is an optional component that handles incoming requests before they reach a listener. Web Application Firewall checks each request for many common threats, based on the Open Web Application Security Project.

Install an internal load balancer.

Install Azure Firewall.

Creating an App Service Plan



App Service Plan Compute Types



The pricing tier of an App Service plan determines the features you get and what you pay. There are three core compute types across the plans.



Shared

Run apps on the same VM as other apps, including apps of other customers.
(Cannot scale out because of shared compute.)



Dedicated

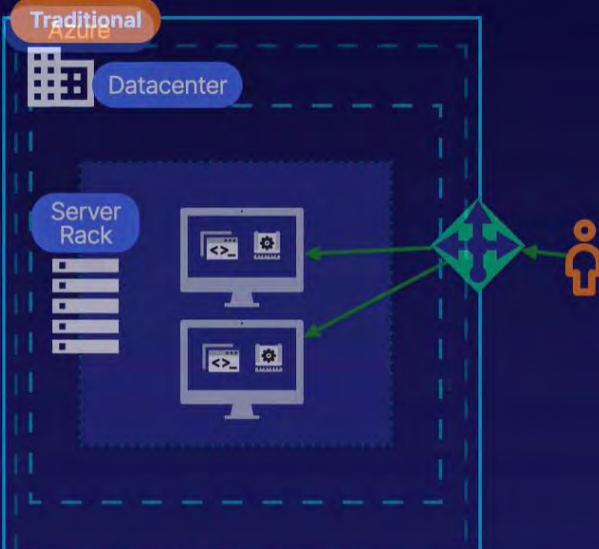
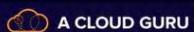
Run only apps using the same App Service Plan on a dedicated VM.
(Isolated compute.)



Isolated

Run apps using dedicated VMs and dedicated VNets.
(Isolated compute and networking.)

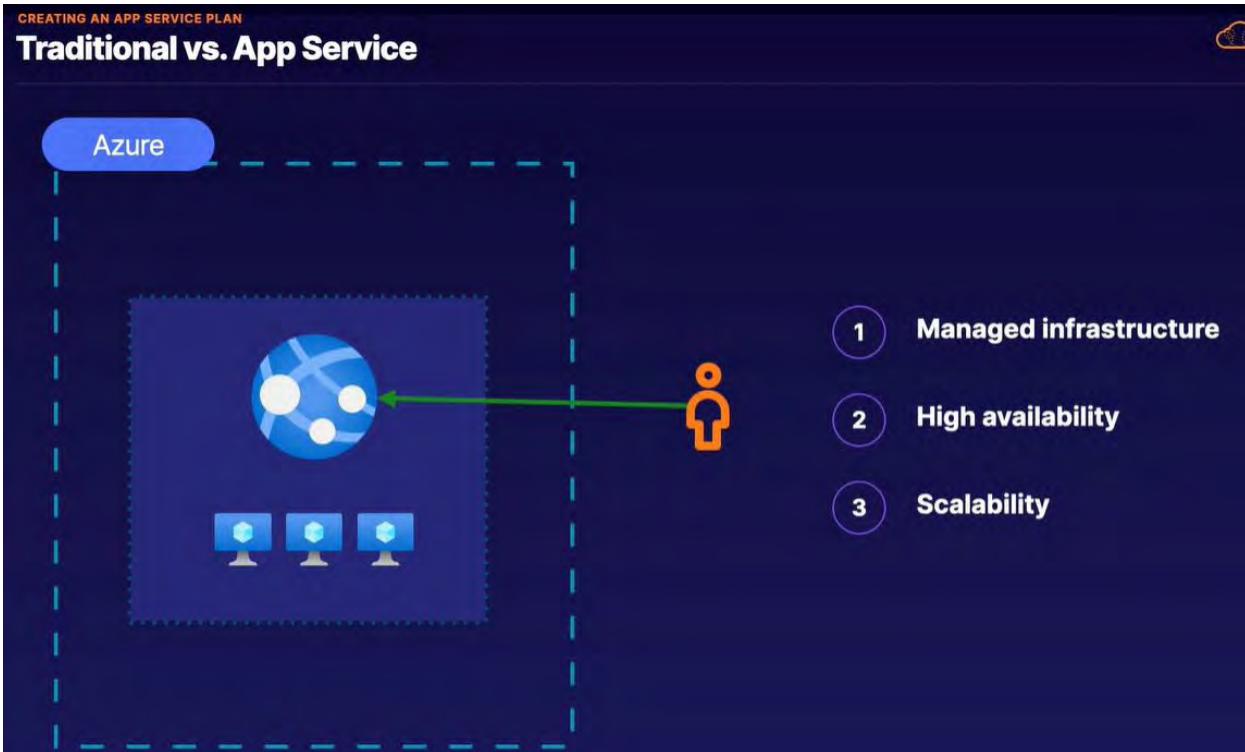
Traditional vs. App Service



- 1 Administer and manage hardware

- 2 Manage patching and security

- 3 Manage load balancing



Para poder crear una web app primero hay que crear un app Service plan

Spec Picker

Dev / Test
For less demanding workloads

Production
For most production workloads

Isolated
Advanced networking and scale

F1 The first Basic (B1) core for Linux is free for the first 30 days!

Recommended pricing tiers

F1 1 GB memory 60 minutes/day compute Free	B1 100 total ACU 1.75 GB memory A-Series compute equivalent 13.14 USD/Month (Estimated)
--	--

See additional options

Included hardware
Every instance of your App Service plan will include the following hardware configuration:

- Memory**
Memory available to run applications deployed and running in the App Service plan.
- Storage**
1 GB disk storage shared by all apps deployed in the App Service plan.

El plan B1 tiene máximo de escalar a 3 instancias la web app

CREATING AN APP SERVICE PLAN

Exam Tips

A CLOUD COMPUTING

App Service Plan

1 App Service Plans
A plan that defines the compute resources and available features for a web app.

2 App Service Plan Compute Resources
Pricing tier, size of VM instances, number of VM instances, and region.

3 App Service Plan Compute Types
Shared, dedicated, and isolated. Each provides a different level of compute isolation, network isolation, and features like scaling.

4 App Service Plans and Web Apps
Provides a Platform as a Service (PaaS) to configure and host applications, rather than managing infrastructure. You just manage a few configuration details and your code.

Implement Azure App Service plans

100 XP

3 minutes

In Azure App Service, an application runs in an Azure App Service plan. An App Service plan defines a set of compute resources for a web application to run. The compute resources are analogous to a server farm in conventional web hosting. One or more applications can be configured to run on the same computing resources (or in the same App Service plan).

Things to know about App Service plans

Let's take a closer look at how to implement and use an App Service plan with your virtual machines.

- When you create an App Service plan in a region, a set of compute resources is created for the plan in the specified region. Any applications that you place into the plan run on the compute resources defined by the plan.
- Each App Service plan defines three settings:
 - Region:** The region for the App Service plan, such as West US, Central India, North Europe, and so on.
 - Number of VM instances:** The number of virtual machine instances to allocate for the plan.
 - Size of VM instances:** The size of the virtual machine instances in the plan, including Small, Medium, or Large.
- You can continue to add new applications to an existing plan as long as the plan has enough resources to handle the increasing load.

How applications run and scale in App Service plans

The Azure App Service plan is the scale unit of App Service applications. Depending on the pricing tier for your Azure App Service plan, your applications run and scale in a different manner. If your plan is configured to run five virtual machine instances, then all applications in the plan run on all five instances. If your plan is configured for autoscaling, then all applications in the plan are scaled out together based on the autoscale settings.

Here's a summary of how applications run and scale in Azure App Service plan pricing tiers:

- Free or Shared tier:**
 - Applications run by receiving CPU minutes on a shared virtual machine instance.
 - Applications can't scale out.
- Basic, Standard, Premium, or Isolated tier:**
 - Applications run on all virtual machine instances configured in the App Service plan.
 - Multiple applications in the same plan share the same virtual machine instances.
 - If you have multiple deployment slots for an application, all deployment slots run on the same virtual machine instances.
 - If you enable diagnostic logs, perform backups, or run WebJobs, these tasks use CPU cycles and memory on the same virtual machine instances.

Things to consider when using App Service plans

Review the following considerations about using Azure App Service plans to run and scale your applications. Think about what conditions might apply to running and scaling the hotel website.

- Consider cost savings. Because you pay for the computing resources that your App Service plan allocates, you can potentially save money by placing multiple applications into the same App Service plan.
- Consider multiple applications in one plan. Create a single plan to support multiple applications, to make it easier to configure and maintain shared virtual machine instances. Because the applications share the same virtual machine instances, you need to carefully manage your plan resources and capacity.
- Consider plan capacity. Before you add a new application to an existing plan, determine the resource requirements for the new application and identify the remaining capacity of your plan.

① Important

Overloading an App Service plan can potentially cause downtime for new and existing applications.

- Consider application isolation. Isolate your application into a new App Service plan when:
 - The application is resource-intensive.
 - You want to scale the application independently from the other applications in the existing plan.
 - The application needs resource in a different geographical region.

Things to know about App Service plan pricing tiers

There are six categories of pricing tiers for an Azure App Service plan. Examine the following plan details and think about which plans can support the hotel website requirements.

Feature	Free	Shared	Basic	Standard	Premium	Isolated
Usage	Development, Testing	Development, Testing	Dedicated development, Testing	Production workloads	Enhanced scale, performance	High performance, security, isolation
Web, mobile, or API applications	10	100	Unlimited	Unlimited	Unlimited	Unlimited
Disk space	1 GB	1 GB	10 GB	50 GB	250 GB	1 TB
Auto scale	n/a	n/a	n/a	Supported	Supported	Supported
Deployment slots	n/a	n/a	n/a	5	20	20
Max instances	n/a	n/a	Up to 3	Up to 10	Up to 30	Up to 100

Free and Shared

The Free and Shared service plans are base tiers that run on the same Azure virtual machines as other applications. Some applications might belong to other customers. These tiers are intended to be used for development and testing purposes only. No SLA is provided for the Free and Shared service plans. Free and Shared plans are metered on a per application basis.

Basic

The Basic service plan is designed for applications that have lower traffic requirements, and don't need advanced auto scale and traffic management features. Pricing is based on the size and number of instances you run. Built-in network load-balancing support automatically distributes traffic across instances. The Basic service plan with Linux runtime environments supports Web App for Containers.

Standard

The Standard service plan is designed for running production workloads. Pricing is based on the size and number of instances you run. Built-in network load-balancing support automatically distributes traffic across instances. The Standard plan includes auto scale that can automatically adjust the number of virtual machine instances running to match your traffic needs. The Standard service plan with Linux runtime environments supports Web App for Containers.

Premium

The Premium service plan is designed to provide enhanced performance for production applications. The upgraded Premium plan, Premium v2, offers Dv2-series virtual machines with faster processors, SSD storage, and double memory-to-core ratio compared to the Standard tier. The new Premium plan also supports higher scale via increased instance count while still providing all the advanced capabilities of the Standard tier. The first generation of Premium plan is still available to support existing customer scaling needs.

Isolated

The Isolated service plan is designed to run mission critical workloads that are required to run in a virtual network. The Isolated plan allows customers to run their applications in a private, dedicated environment in an Azure datacenter. The plan offers Dv2-series virtual machines with faster processors, SSD storage, and a double memory-to-core ratio compared to the Standard tier. The private environment used with an Isolated plan is called the App Service Environment. The plan can scale to 100 instances with more available upon request.

Things to know about Azure App Service scaling

Let's examine the details of scaling for your Azure App Service plan and App Service applications.

- The scale up method increases the amount of CPU, memory, and disk space. Scaling up gives you extra features like dedicated virtual machines, custom domains and certificates, staging slots, autoscaling, and more. You scale up by changing the pricing tier of the Azure App Service plan where your application is placed.
- The scale-out method increases the number of virtual machine instances that run your application. You can scale out to as many as 30 instances, depending on your App Service plan pricing tier. Take advantage of App Service Environments in the Isolated tier to further increase your scale-out count to 100 instances. The scale instance count can be configured manually or automatically (autoscale).
- With autoscale, you can automatically increase the scale instance count for the scale-out method. Autoscale is based on predefined rules and schedules.
- Your App Service plan can be scaled up and down at any time by changing the pricing tier of the plan.

Things to consider when using Azure App Service scaling

Review the following benefits of implementing scaling for your App Service plan and applications. Think about the scaling advantages for your hotel website.

- Consider manually adjusting plan tiers. Start your plan at a lower pricing tier and scale up as needed to acquire more App Service features. Scale down when features are no longer needed, and control your overall costs.

Consider a scenario where you start testing your web app by using the Azure App Service Free tier, where you pay nothing to use the service. After a while, you decide to add a custom DNS name to your web app, so you scale your plan up to the Shared tier. Next, you discover you need to create an SSL binding, so you scale your plan up to the Basic tier. Later, you determine a need for staging environments, so you scale up to the Standard tier. When you need more cores, memory, or storage, you can scale up to a bigger virtual machine size in the same tier.

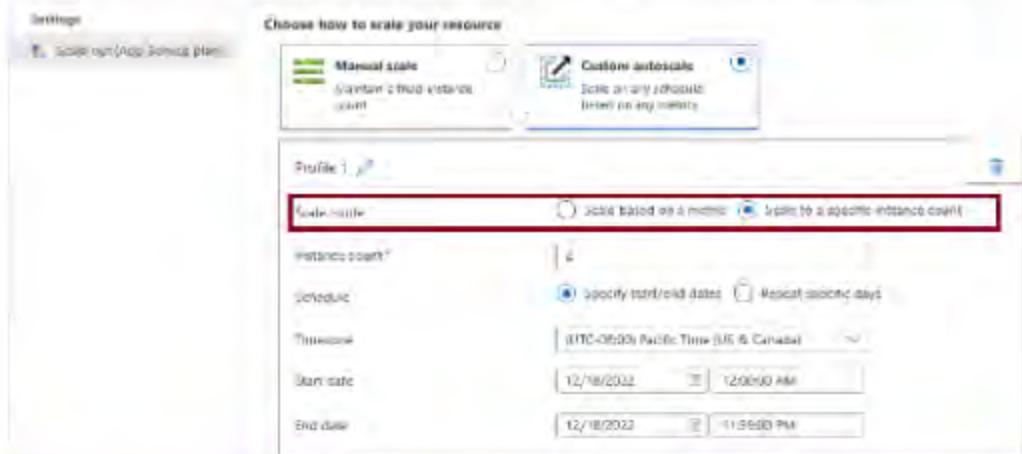
The same scaling process works in reverse. If you decide you no longer need capabilities or features of a higher tier, scale your plan down to a lower tier and save money.

- Consider autoscale to support users and reduce costs. Keep serving your users when your application is experiencing high throughput. Implement autoscale to control how many features and support are offered at a given time based on your preference settings and rule conditions. Autoscale helps you save money when the load on your application decreases by automatically reducing your subscribed features.
- Consider no redeployment. When you change your scale settings, you don't need to change your code or redeploy your applications. Changing your plan scale settings takes only seconds to apply. Your changes affect all applications in your App Service plan.
- Consider scaling for other Azure services. If your App Service application depends on other Azure services, such as Azure SQL Database or Azure Storage, you can scale these resources separately. These resources aren't managed by your App Service plan.

Things to know about autoscale

Let's take a closer look at how to use autoscale for your Azure App Service plan and applications.

- To use autoscale, you specify the minimum, and maximum number of instances to run by using a set of rules and conditions.
- When your application runs under autoscale conditions, the number of virtual machine instances are automatically adjusted based on your rules. When rule conditions are met, one or more autoscale actions are triggered.
- An autoscale setting is read by the autoscale engine to determine whether to scale out or in. Autoscale settings are grouped into profiles.
- Autoscale rules include a trigger and a scale action (in or out). The trigger can be metric-based or time-based.



- Metric-based rules measure application load and add or remove virtual machines based on the load, such as "do this action when CPU usage is above 50%." Example metrics include CPU time, Average response time, and Requests.
- Time-based rules (or, schedule-based) allow you to scale when you see time patterns in your load and want to scale before a possible load increase or decrease occurs. An example is "trigger a webhook every 8:00 AM on Saturday in a given time zone."
- The autoscale engine uses notification settings.

A notification setting defines what notifications should occur when an autoscale event occurs based on satisfying the criteria of an autoscale setting profile. Autoscale can notify one or more email addresses or make calls to one or more webhooks.

Things to consider when configuring autoscale

There are several considerations to keep in mind when you configure autoscale for your Azure App Service plan and applications.

- **Minimum instance count.** Set a minimum instance count to make sure your application is always running even when there's no load.
- **Maximum instance count.** Set a maximum instance count to limit your total possible hourly cost.
- **Adequate scale margin.** Make sure your maximum and minimum instance count values are different, and set an adequate margin between the two values. You can automatically scale between the minimum and maximum by using rules you create.
- **Scale rule combinations.** Always use a scale-out and scale-in rule combination that performs an increase and decrease. If you don't set a scale-out rule, your application might fail, or performance might degrade under increased loads. If you don't set a scale-in rule, you can experience unnecessary and extensive costs when the load decreases.
- **Metric statistics.** Carefully choose the appropriate statistic for your diagnostic metrics, including Average, Minimum, Maximum, and Total.
- **Default instance count.** Always select a safe default instance count. The default instance count is important because autoscale scales your service to the count you specify when metrics aren't available.
- **Notifications.** Always configure autoscale notifications. It's important to maintain awareness of how your application is performing as the load changes.

1. Which App Service Plan can you implement to support the Production team's requirements? *

- Basic
 Standard
 Premium

✓ Correct. The Premium App Service plan meets the requirements of scaling to 5 instances and 100 GB of disk storage.

2. What scaling option provides more CPU, memory, or disk space without adding more virtual machines? *

- Scale up
 Scale out
 Scale back

✓ Correct. Scale up gives more CPU, memory, and disk space. You can scale up by changing the pricing tier of the App Service plan.

3. Triggering a webhook at 8:00 AM on Saturday is an example of what type of rule? *

- A metric-based rule.
 A time-based rule.
 An app-insight rule.

✓ Correct. Time-based rules allow scaling based on time patterns.

Implement Azure App Service

✓ 100 XP

2 minutes

Azure App Service brings together everything you need to create websites, mobile backends, and web APIs for any platform or device. Applications run and scale with ease in both Windows and Linux-based environments.

App Service provides Quickstarts for several products to help you easily create and deploy your Windows and Linux apps:



ASP.NET



Java



Node.js



PHP



HTML



Ruby



WordPress



Custom containers (Windows or Linux)



Python on Linux (Django or Flask)

App Service benefits

There are many advantages to using App Service to develop and deploy your web, mobile, and API apps. Review the following table and think about what features can help you host your App Service instances.

Benefit	Description
Multiple languages and frameworks	App Service has first-class support for ASP.NET, Java, Ruby, Node.js, PHP, and Python. You can also run PowerShell and other scripts or executables as background services.
DevOps optimization	App Service supports continuous integration and deployment with Azure DevOps, GitHub, BitBucket, Docker Hub, and Azure Container Registry. You can promote updates through test and staging environments. Manage your apps in App Service by using Azure PowerShell or the cross-platform command-line interface (CLI).
Global scale with high availability	App Service helps you scale up or out manually or automatically. You can host your apps anywhere within the Microsoft global datacenter infrastructure, and the App Service SLA offers high availability.
Connections to SaaS platforms and on-premises data	App Service lets you choose from more than 50 connectors for enterprise systems (such as SAP), SaaS services (such as Salesforce), and internet services (such as Facebook). You can access on-premises data by using Hybrid Connections and Azure Virtual Networks.
Security and compliance	App Service is ISO, SOC, and PCI compliant. You can authenticate users with Azure Active Directory or with social logins via Google, Facebook, Twitter, or Microsoft. Create IP address restrictions and manage service identities.
Application templates	Choose from an extensive list of application templates in the Azure Marketplace, such as WordPress, Joomla, and Drupal.
Visual Studio integration	App Service offers dedicated tools in Visual Studio to help streamline the work of creating, deploying, and debugging.
API and mobile features	App Service provides turn-key CORS support for RESTful API scenarios. You can simplify your mobile app scenarios by enabling authentication, offline data sync, push notifications, and more.
Serverless code	App Service lets you run a code snippet or script on-demand without having to explicitly provision or manage infrastructure. You pay only for the compute time your code actually uses.

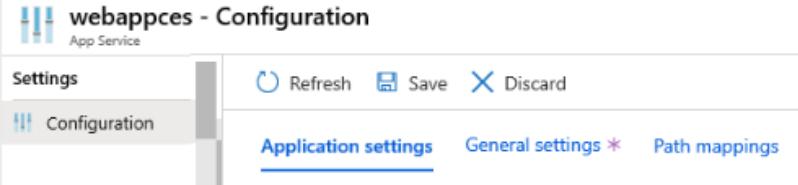
Things to know about configuration settings

Let's examine some of the basic configuration settings you need to create an app with App Service.

- Name: The name for your app must be unique because it's used to identify and locate your app in Azure. An example name is `webappces1.azurewebsites.net`. You can map a custom domain name, if you prefer to use that option instead.
- Publish: App Service hosts (publishes) your app as code or as a Docker Container.
- Runtime stack: App Service uses a software stack to run your app, including the language and SDK versions. For Linux apps and custom container apps, you can set an optional start-up command or file. Your choices for the stack include .NET Core, .NET Framework, Node.js, PHP, Python, and Ruby. Various versions of each product are available for Linux and Windows.
- Operating system: The operating system for your app runtime stack can be Linux or Windows.
- Region: The region location that you choose for your app affects the App Service plans that are available.
- App Service plan: Your app needs to be associated with an Azure App Service plan to establish available resources, features, and capacity. You can choose from pricing tiers that are available for the region location you selected.

Post-creation settings

After your app is created, other configuration settings become available in the Azure portal, including app deployment options and path mapping.



The screenshot shows the Azure portal's Configuration blade for an App Service named "webappces". The "Configuration" tab is selected. At the top, there are buttons for Refresh, Save, and Discard. Below the tabs, there are sections for Application settings, General settings, and Path mappings.

Some of the extra configuration settings can be included in the developer's code, while others can be configured in your app. Here are a few of the extra application settings.

- Always On: You can keep your app loaded even when there's no traffic. This setting is required for continuous WebJobs or for WebJobs that are triggered by using a CRON expression.
- ARR affinity: In a multi-instance deployment, you can ensure your app client is routed to the same instance for the life of the session.
- Connection strings: Connection strings for your app are encrypted at rest and transmitted over an encrypted channel.

Things to know about continuous deployment

When you create your web app with App Service, you can choose automated or manual deployment. As you review these options, consider which deployment method to implement for your App Service apps.

- Automated deployment (continuous integration) is a process used to push out new features and bug fixes in a fast and repetitive pattern with minimal impact on end users. Azure supports automated deployment directly from several sources:
 - Azure DevOps: Push your code to Azure DevOps (previously known as Visual Studio Team Services), build your code in the cloud, run the tests, generate a release from the code, and finally, push your code to an Azure web app.
 - GitHub: Azure supports automated deployment directly from GitHub. When you connect your GitHub repository to Azure for automated deployment, any changes you push to your production branch on GitHub are automatically deployed for you.
 - Bitbucket: With its similarities to GitHub, you can configure an automated deployment with Bitbucket.
- Manual deployment enables you to manually push your code to Azure. There are several options for manually pushing your code:
 - Git: The App Service Web Apps feature offers a Git URL that you can add as a remote repository. Pushing to the remote repository deploys your app.
 - CLI: The `webapp up` command is a feature of the command-line interface that packages your app and deploys it. Deployment can include creating a new App Service web app.
 - Visual Studio: Visual Studio features an App Service deployment wizard that can walk you through the deployment process.
 - FTP/S: FTP or FTPS is a traditional way of pushing your code to many hosting environments, including App Service.

Things to know about deployment slots

Let's take a closer look at the characteristics of deployment slots.

- Deployment slots are live apps that have their own hostnames.
- Deployment slots are available in the Standard, Premium, and Isolated App Service pricing tiers. Your app needs to be running in one of these tiers to use deployment slots.
- The Standard, Premium, and Isolated tiers offer different numbers of deployment slots.
- App content and configuration elements can be swapped between two deployment slots, including the production slot.

The screenshot shows the Azure portal interface for managing deployment slots. At the top, there are buttons for 'Save', 'Discard', 'Add Slot', 'Swap', 'Logs', and 'Refresh'. Below this, a section titled 'Deployment Slots' displays the following information:

Deployment slots are live apps with their own hostnames. App content and configurations can be swapped between two deployment slots, including the production slot.

NAME	STATUS	APP SERVICE PLAN	TRAFFIC %
webappces PRODUCTION	Running	ASP-webapprg-a247	<div style="width: 100%;">100</div>
webappces-Staging	Running	ASP-webapprg-a247	<div style="width: 0%;">0</div>

Things to consider when using deployment slots

There are several advantages to using deployment slots with your App Service app. Review the following benefits and think about how they can support your App Service implementation.

- Consider validation. You can validate changes to your app in a staging deployment slot before swapping the app changes with the content in the production slot.
- Consider reductions in downtime. Deploying an app to a slot first and swapping it into production ensures that all instances of the slot are warmed up before being swapped into production. This option eliminates downtime when you deploy your app. The traffic redirection is seamless, and no requests are dropped because of swap operations. The entire workflow can be automated by configuring Auto swap when pre-swap validation isn't needed.
- Consider restoring to last known good site. After a swap, the slot with the previously staged app now has the previous production app. If the changes swapped into the production slot aren't as you expected, you can perform the same swap immediately to return to your "last known good site."
- Consider Auto swap. Auto swap streamlines Azure DevOps scenarios where you want to deploy your app continuously with zero cold starts and zero downtime for app customers. When Auto-swap is enabled from a slot into production, every time you push your code changes to that slot, App Service automatically swaps the app into production after it's warmed up in the source slot. Auto swap isn't currently supported for Web Apps on Linux.

Things to know about creating deployment slots

Let's review some details about how deployment slots are configured.

- New deployment slots can be empty or cloned.
- Deployment slot settings fall into three categories:
 - Slot-specific app settings and connection strings (if applicable)
 - Continuous deployment settings (when enabled)
 - Azure App Service authentication settings (when enabled)
- When you clone a configuration from another deployment slot, the cloned configuration is editable. Some configuration elements follow the content across the swap. Other slot-specific configuration elements stay in the source slot after the swap.

Swapped settings versus slot-specific settings

The following table lists the settings that are swapped between deployment slots, and settings that remain in the source slot (slot-specific). As you review these settings, consider which features are required for your App Service apps.

Swapped settings	Slot-specific settings
General settings, such as framework version, 32/64-bit, web sockets	Custom domain names
App settings *	Non-public certificates and TLS/SSL settings
Connection strings *	Scale settings
Handler mappings	Always On
Public certificates	IP restrictions
WebJobs content	WebJobs schedulers
Hybrid connections **	Diagnostic settings
Service endpoints **	Cross-origin resource sharing (CORS)
Azure Content Delivery Network **	Virtual network integration
Path mapping	Managed identities
	Settings that end with the suffix _EXTENSION_VERSION

* Setting can be configured to be slot-specific.

** Feature isn't currently available.

Secure your App Service app

✓ 100 XP

3 minutes

Azure App Service provides built-in authentication and authorization support. You can sign in users and access data by writing minimal or no code in your web app, API, and mobile backend, and also your Azure Functions apps.

Secure authentication and authorization require deep understanding of security, including federation, encryption, JSON web tokens (JWT) management, grant types, and so on. App Service provides these utilities so you can spend more time and energy on providing business value to your customer.

Note

You aren't required to use Azure App Service for authentication and authorization. Many web frameworks are bundled with security features, and you can use your preferred service.

Things to know about app security with App Service

Let's take a closer look at how App Service helps you provide security for your app.

- The authentication and authorization security module in Azure App Service runs in the same environment as your application code, yet separately.
- The security module is configured by using app settings. No SDKs, specific languages, or changes to your application code are required.
- When you enable the security module, every incoming HTTP request passes through the module before it's handled by your application code.
- The security module handles several tasks for your app:
 - Authenticate users with the specified provider
 - Validate, store, and refresh tokens
 - Manage the authenticated session
 - Inject identity information into request headers

Things to consider when using App Service for app security

You configure authentication and authorization security in App Service by selecting features in the Azure portal. Review the following options and think about what security can benefit your App Service apps implementation.

- Allow Anonymous requests (no action). Defer authorization of unauthenticated traffic to your application code. For authenticated requests, App Service also passes along authentication information in the HTTP headers. This feature provides more flexibility for handling anonymous requests. With this feature, you can present multiple sign-in providers to your users.
- Allow only authenticated requests. Redirect all anonymous requests to `/auth/login/<provider>` for the provider you choose. The feature is equivalent to Log in with `<provider>`. If the anonymous request comes from a native mobile app, the returned response is an `HTTP 401 Unauthorized` message. With this feature, you don't need to write any authentication code in your app.

Important

This feature restricts access to all calls to your app. Restricting access to all calls might not be desirable if your app requires a public home page, as is the case for many single-page apps.

- Logging and tracing. View authentication and authorization traces directly in your log files. If you see an authentication error that you didn't expect, you can conveniently find all the details by looking in your existing application logs. If you enable failed request tracing, you can see exactly how the security module participated in a failed request. In the trace logs, look for references to a module named `EasyAuthModule_32/64`.

Configure a custom domain name for your app

There are three steps to create a custom domain name. The following steps outline how to create a domain name in the Azure portal.

ⓘ Important

To map a custom DNS name to your app, you need a paid tier of an App Service plan for your app.

1. Reserve your domain name. If you haven't registered for an external domain name for your app, the easiest way to set up a custom domain is to buy one directly in the Azure portal. (This name isn't the Azure assigned name of `*.azurewebsites.net`.) The registration process enables you to manage your web app's domain name directly in the Azure portal instead of going to a third-party site. Configuring the domain name in your web app is also a simple process in the Azure portal.
2. Create DNS records to map the domain to your Azure web app. The Domain Name System (DNS) uses data records to map domain names to IP addresses. There are several types of DNS records.
 - For web apps, you create either an `A` (Address) record or a `CNAME` (Canonical Name) record.
 - An `A` record maps a domain name to an IP address.
 - A `CNAME` record maps a domain name to another domain name. DNS uses the second name to look up the address. Users still see the first domain name in their browser. As an example, you could map `contoso.com` to your `webapp.azurewebsites.net` URL.
 - If the IP address changes, a `CNAME` entry is still valid, whereas an `A` record must be updated.
 - Some domain registrars don't allow `CNAME` records for the root domain or for wildcard domains. In such cases, you must use an `A` record.
3. Enable the custom domain. After you have your domain and create your DNS record, use the Azure portal to validate your custom domain and add it to your web app. Be sure to test your domain before publishing.

Things to know about Backup and Restore

Examine the following details about the Backup and Restore feature. Think about how you can implement this feature for your App Service apps.

- To use the Backup and Restore feature, you need the Standard or Premium tier App Service plan for your app or site.
- You need an Azure storage account and container in the same subscription as the app to back up.
- Azure App Service can back up the following information to the Azure storage account and container you configured for your app:
 - App configuration settings
 - File content
 - Any database connected to your app (SQL Database, Azure Database for MySQL, Azure Database for PostgreSQL, MySQL in-app)
- In your storage account, each backup consists of a Zip file and XML file:
 - The Zip file contains the back-up data for your app or site.
 - The XML file contains a manifest of the Zip file contents.
- You can configure backups manually or on a schedule.
- Full backups are the default.
- Partial backups are supported. You can specify files and folders to exclude from a backup.
- You restore partial backups of your app or site the same way you restore a regular backup.
- Backups can hold up to 10 GB of app and database content.
- Backups for your app or site are visible on the Containers page of your storage account and app (or site) in the Azure portal.

Things to consider when creating backups and restoring backups

Let's review some considerations about creating a backup for your app or site, and restoring data and content from a backup.

- Consider full backups. Do a full backup to easily save all configuration settings, all file content, and all database content connected with your app or site.

When you restore a full backup, all content on the site is replaced with whatever is in the backup. If a file is on the site, but not in the backup, the file is deleted.

- Consider partial backups. Specify a partial backup so you can choose exactly which files to back up.

When you restore a partial backup, any content located in an excluded folder or file is left as-is.

- Consider browsing back-up files. Unzip and browse the Zip and XML files associated with your backup to access your backups. This option lets you view the content without actually performing an app or site restore.
- Consider firewall on back-up destination. If your storage account is enabled with a firewall, you can't use the storage account as the destination for your backups.

Use Azure Application Insights

100 XP

3 minutes

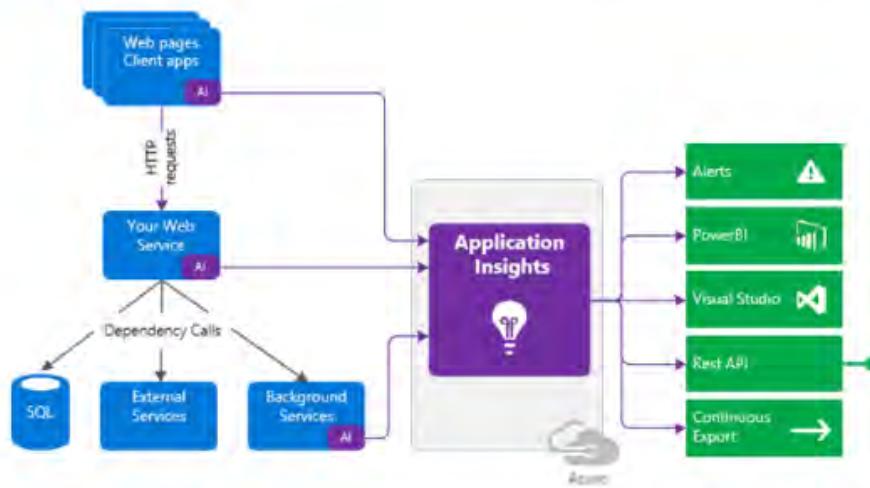
Azure Application Insights is a feature of Azure Monitor that lets you monitor your live applications. You can integrate Application Insights with your App Service configure to automatically detect performance anomalies in your apps.

Application Insights is designed to help you continuously improve the performance and usability of your apps. The feature offers powerful analytics tools to help you diagnose issues and understand what users actually do with your apps.

Things to know about Application Insights

Let's examine some characteristics of Application Insights for Azure Monitor.

- Application Insights works on various platforms including .NET, Node.js and Java EE.
- The feature can be used for configurations that are hosted on-premises, in a hybrid environment, or in any public cloud.
- Application Insights integrates with your Azure DevOps process, and has connection points to many development tools.
- You can monitor and analyze data from mobile apps by integrating with Visual Studio App Center.



Things to consider when using Application Insights

Application Insights is ideal for supporting your development team. The feature helps developers understand how your app is performing and how it's being used. Consider monitoring the following items in your App Service configuration scenario.

- Consider Request rates, response times, and failure rates. Find out which pages are most popular, at what times of day, and where your users are. See which pages perform best. If your response times and failure rates go high when there are more requests, then perhaps you have a resourcing problem.
- Consider Dependency rates, response times, and failure rates. Use Application Insights to discover if external services are degrading your app performance.
- Consider Exceptions. Analyze the aggregated statistics, or pick specific instances and drill into the stack trace and related requests. Both server and browser exceptions are reported.
- Consider Page views and load performance. Collect the number of page views reported by your users' browsers and analyze the load performance.
- Consider User and session counts. Application Insights can help you keep track of the number of users and sessions connected to your app.
- Consider Performance counters. Add Application Insights performance counters from your Windows or Linux server machines. Monitor performance output for the CPU, memory, network usage, and so on.
- Consider Host diagnostics. Integrate diagnostics from Docker or Azure into your app Application Insights.
- Consider Diagnostic trace logs. Implement trace logs from your app to help correlate trace events with requests and diagnose issues.
- Consider Custom events and metrics. Write your own custom events and metric tracking algorithms as client or server code. Track business events such as number of items sold, or number of games won.

1. When you clone a configuration from another deployment slot, which configuration setting follows the content across the swap? *

Custom domain names

Connection strings

✓ Correct. Connections strings follow the content across the swap.

Scale settings

2. How can you support the Marketing team requests about research web page usage? *

Continuous deployment

Application logging

Azure Application insights

✓ Correct. Application Insights meets all the requirements. The product can also determine which web pages perform best.

3. Which option is a valid automated deployment source? *

GitHub

✓ Correct. Azure currently supports Azure DevOps, GitHub, Bitbucket, OneDrive, Dropbox, and external Git repositories.

JavaScript code

SharePoint

Creating Web Apps

**Managed Infrastructure**

No need to patch, maintain, implement, or configure underlying infrastructure components with this Platform as a Service (PaaS).

**Development Focused**

Development of application code is the focus for web app service deployments.

**Highly Available**

Azure App Service runs apps on multiple nodes to provide high availability.

**Deployment Slots**

CI/CD DevOps provides features such as staging slots for deployments, e.g. production slot and staging slot.

**Autoscaling In/Out**

Scaling capabilities similar to scale sets ensure you can meet the traffic demands of your application.

**Azure Service Integration**

App Service integrates several Azure services, such as Azure AD as an identity provider or VNets for connecting App Service to resources within a virtual network.

Podemos hacer continuos deployment se usa un zip o github actions

Desplegar una web app:

```
Powershell > PS /home/cloud/demowebapp/pub> az webapp deployment source config-zip `>> --src ./site.zip `>> --resource-group $rg `>> --name $appname
```

Web Apps

1 Application Runtime

Host an application using a specific runtime that is selected as part of the provisioning process.

2 Public Accessibility

Web Apps are publicly accessible by default, and can be accessed using the domain provided to you by Azure.

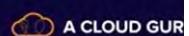
3 Publishing Tools

Publish your application code to web apps using various publishing tools including Azure DevOps, GitHub, Zip file, SCM, etc.

4 Database Support

Connect your database to your web app using a connection string.

Configuration Options



Custom Domain

Provide a custom domain to be used by the web application. For example, www.acloudguru.com.

01

02

Scaling

Specify scaling options to scale up/scale out compute resources for your web apps.

Backup

Back up web apps using full archival backups or incremental snapshots that are stored in a storage account via the Blob Storage Service.

05

03

Deployment

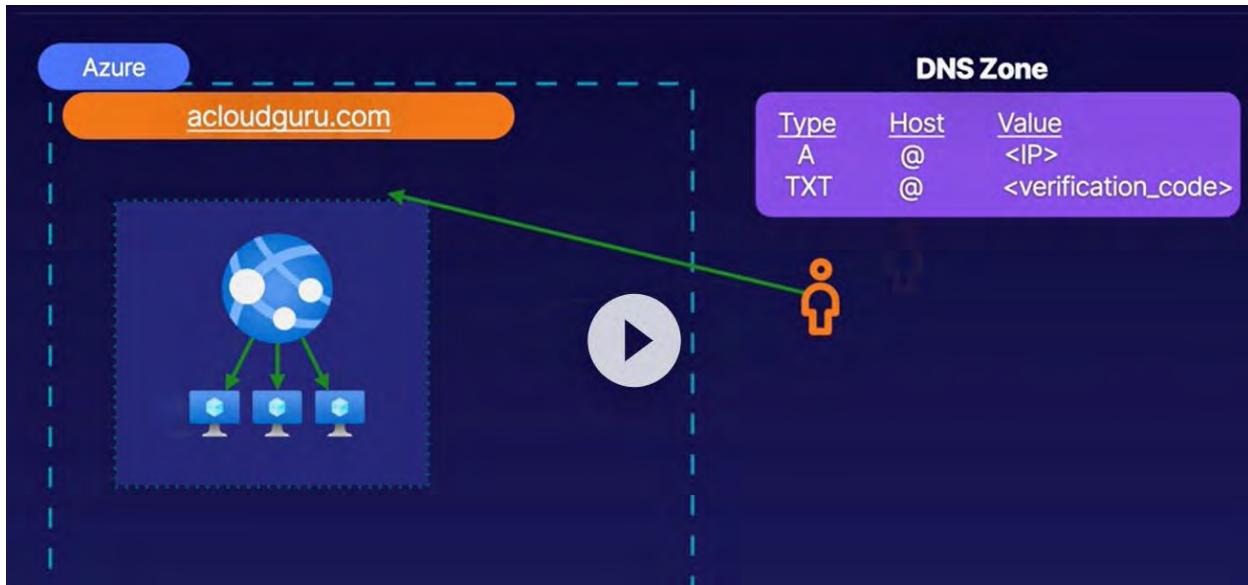
Deploy applications using DevOps strategies like deployment slots for a staging slot and a production slot.

04

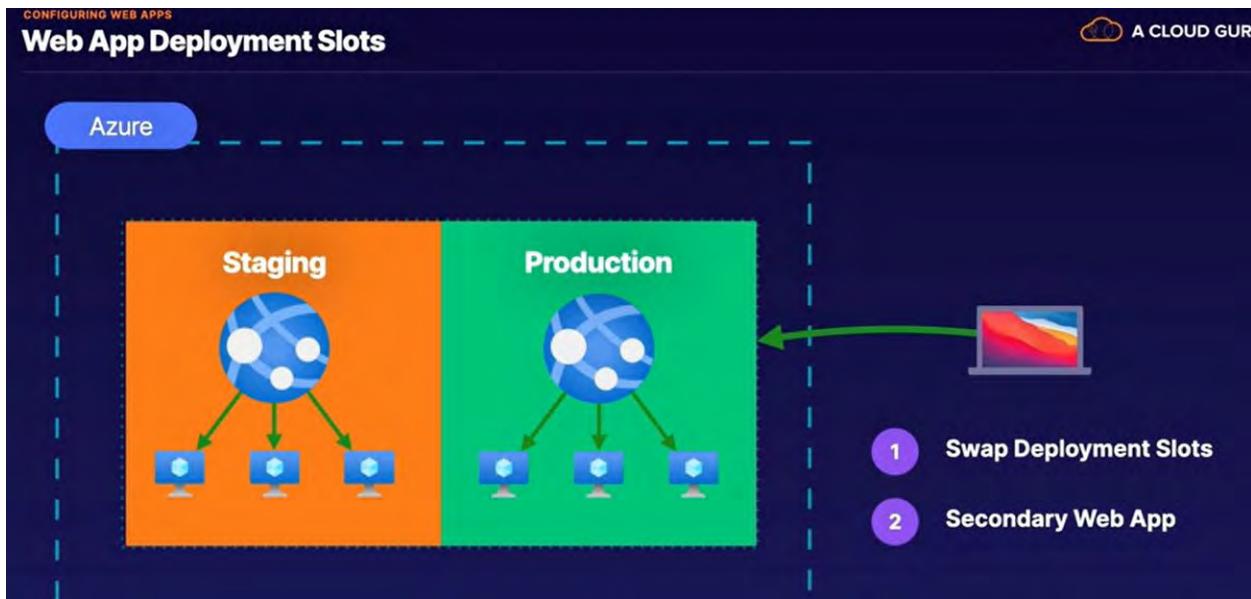
Network

Manage network settings and integration by doing things such as connecting web apps with VNets, CDN, etc.

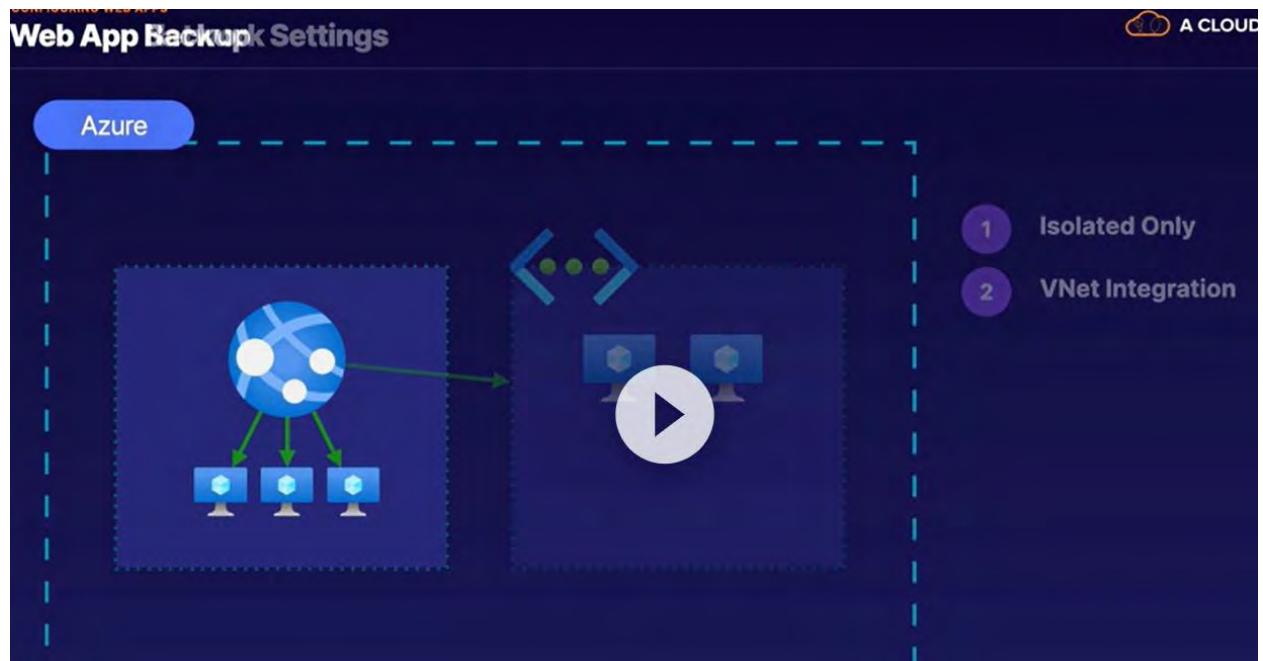
Para tener un custom domain tenemos que poner el código de verificación de que ese dominio nos pertenece



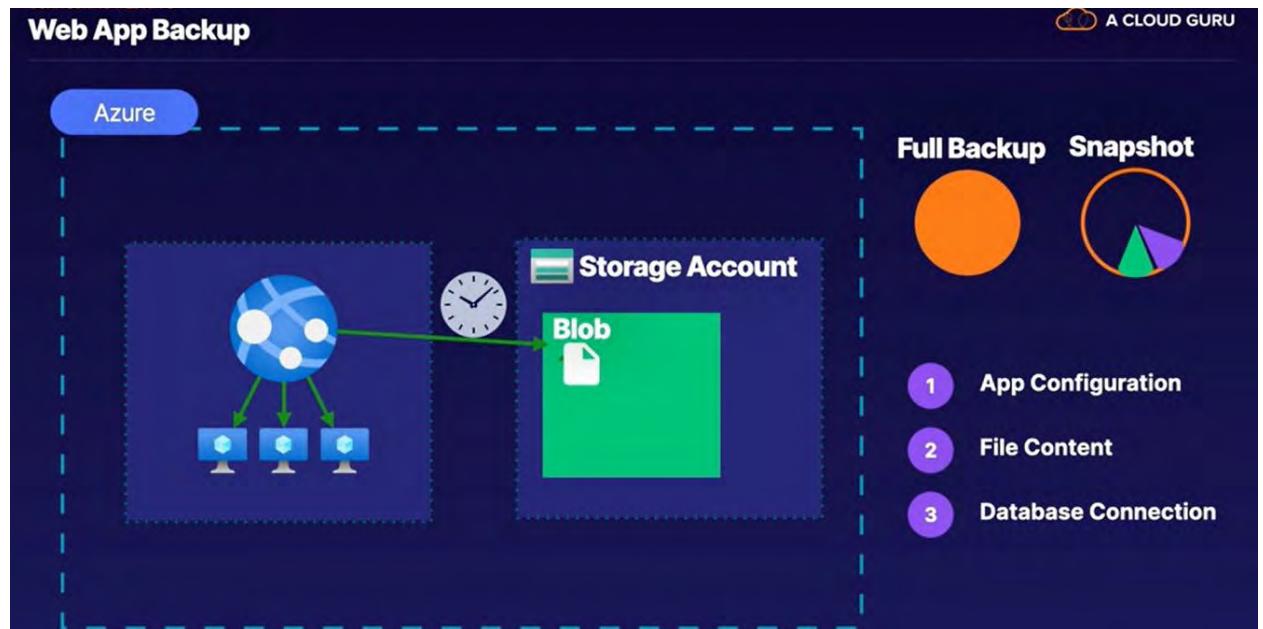
Los deployment slots son para tener dos web apps, la segunda viene sin costo y podemos por ejemplo tener un staging y luego hacer swap entre ambientes para definir cual es producción,



Las web apps son accesibles públicamente por default.



Para el backup de nuestra web app podemos definir un blob storage para que haga backup completo o también snapshots



Para usar los slots es necesario un plan standard o premium



Upgrade to a standard or premium plan to add slots.

Deployment slots are live apps with their own hostnames. App content and configurations elements can be swapped between two deployment slots, including the production slot. [Learn more](#)

[Upgrade](#)

Puedes autenticar por medio de azure ad

Ejemplo de custom domain

Add custom domain

X

cloudchasewebappdemo

domain verification id below. [Learn More](#)

Custom Domain Verification ID:

71E0697E215335964F9E08587D945527C939AB4C4126DD0...

External IP address

52.176.2.229

[Add custom domain](#)

DNS propagation

Please be aware that depending on your DNS provider it can take up to 48 hours for the DNS entry changes to propagate. You can verify that the DNS propagation is working as expected by using <https://digwebinterface.com/>. [Learn more](#)

Hostname availability

Domain ownership

To verify domain ownership create TXT and A records with your DNS provider using the configuration below. [Learn more](#)

Type Host Value

TXT asuid 71E0697E215335964F9E08587D945527C939AB4C4126C

A @ 52.176.2.229

DEVELOP YOUR APP WITH NETWORKING

App Service

SSH (Cmd+J)
System logs

Payment Center

Configuration

Entitlement

Entitlement (classic)

Application Insights

Identity

Logs

Custom domains

SSL settings

Working

Setup (App Service plan)

Output (App Service plan)

Jobs



VNet Integration

Securely access resources available in or through your Azure VNet.
[Learn More](#)

[Click here to configure](#)



Hybrid connections

Securely access applications in private networks
[Learn More](#)

[Configure your hybrid connection endpoints](#)



Azure Front Door with Web Application Firewall

Scalable and secure entry point for accelerated delivery of your web applications
[Learn More](#)

[Configure Azure Front Door with WAF for your app](#)



Azure CDN

Secure, reliable content delivery with broad global reach and rich feature set
[Learn More](#)



Azure CDN

Secure, reliable content delivery with broad global reach and rich feature set
[Learn More](#)

[Configure Azure CDN for your app](#)



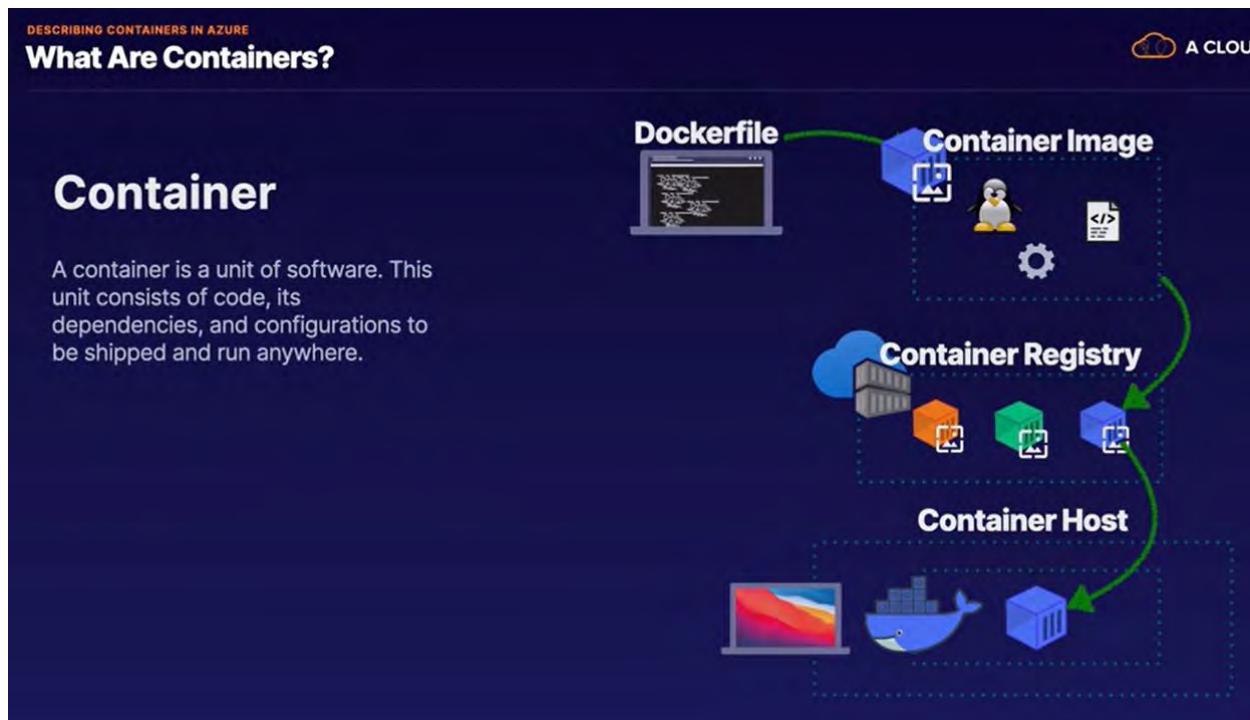
Access Restrictions

Define and manage rules that control access to your application.
[Learn More](#)

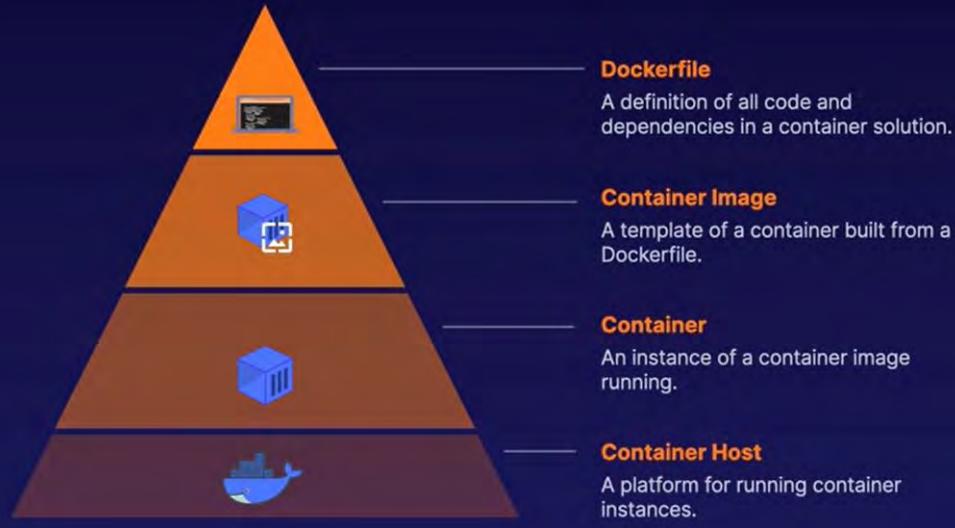
[Configure Access Restrictions](#)



Describing containers in Azure



What Are Containers?



Si queremos hacer un push a docker container registry

```
cloudchase@cloudchase-VirtualBox:~/Desktop/projects/containerdemo$ docker login cloudchasereregdemo.azurecr.io --username cloudchasereregdemo
Password:
WARNING! Your password will be stored unencrypted in /home/cloudchase/.docker/config.json.
Configure a credential helper to remove this warning. See
https://docs.docker.com/engine/reference/commandline/login/#credentials-store

Login Succeeded
cloudchase@cloudchase-VirtualBox:~/Desktop/projects/containerdemo$ docker tag containerdemo cloudchase regdemo.azurecr.io/myimages/containerdemo:latest
cloudchase@cloudchase-VirtualBox:~/Desktop/projects/containerdemo$ docker push cloudchasereregdemo.azurecr.io/myimages/containerdemo:latest
The push refers to repository [cloudchasereregdemo.azurecr.io/myimages/containerdemo]
9ebc2f5090a0: Pushed
fa728254b20e: Pushed
b3a48e9ca2ba: Pushed
8aad4316c1e3: Pushed
9f7793952dca: Pushed
2bb84c5f5766: Waiting
8ea3b23f387b: Waiting
```

Compare containers to virtual machines

 100 XP

3 minutes

Hardware virtualization has made it possible to run multiple isolated instances of operating systems concurrently on the same physical hardware. Containers represent the next stage in the virtualization of computing resources.

Container-based virtualization allows you to virtualize the operating system. This approach lets you run multiple applications within the same instance of an operating system, while maintaining isolation between the applications. The containers within a virtual machine provide functionality similar to that of virtual machines within a physical server.

Things to know about containers versus virtual machines

To better understand container-based virtualization, let's compare containers and virtual machines.

Compare	Containers	Virtual machines
Isolation	A container typically provides lightweight isolation from the host and other containers, but a container doesn't provide as strong a security boundary as a virtual machine.	A virtual machine provides complete isolation from the host operating system and other virtual machines. This separation is useful when a strong security boundary is critical, such as hosting apps from competing companies on the same server or cluster.
Operating system	Containers run the user mode portion of an operating system and can be tailored to contain just the needed services for your app. This approach helps you use fewer system resources.	Virtual machines run a complete operating system including the kernel, which requires more system resources (CPU, memory, and storage).
Deployment	You can deploy individual containers by using Docker via the command line. You can deploy multiple containers by using an orchestrator such as Azure Kubernetes Service.	You can deploy individual virtual machines by using Windows Admin Center or Hyper-V Manager. You can deploy multiple virtual machines by using PowerShell or System Center Virtual Machine Manager.
Persistent storage	Containers use Azure Disks for local storage for a single node, or Azure Files (SMB shares) for storage shared by multiple nodes or servers.	Virtual machines use a virtual hard disk (VHD) for local storage for a single machine, or an SMB file share for storage shared by multiple servers.
Fault tolerance	If a cluster node fails, any containers running on the node are rapidly recreated by the orchestrator on another cluster node.	Virtual machines can fail over to another server in a cluster, where the virtual machine's operating system restarts on the new server.

Things to consider when using containers

Containers offer several advantages over physical and virtual machines. Review the following benefits and consider how you can implement containers for the internal apps for your company.

- Consider flexibility and speed. Gain increased flexibility and speed when developing and sharing your containerized application code.
- Consider testing. Choose containers for your configuration to allow for simplified testing of your apps.
- Consider app deployment. Implement containers to gain streamlined and accelerated deployment of your apps.
- Consider workload density. Support higher workload density and improve your resource utilization by working with containers.

Using Azure container instances for containers

USING AZURE CONTAINER INSTANCES FOR CONTAINERS

Describing Azure Container Instances

The diagram illustrates the concept of Azure Container Instances. At the top, a blue cloud icon with an upward arrow is labeled "Azure Container Instances". Below it, a dashed-line box represents a "Container Group". Inside this group, there are two separate sections. The first section contains one blue cube icon, and the second section contains two blue cube icons. Arrows point from each section to a small computer monitor icon at the bottom, representing local networking and storage.

Defining Container Groups

A collection of containers that share a lifecycle, resources, local networking, and storage.

USING AZURE CONTAINER INSTANCES FOR CONTAINERS

Describing Azure Container Instances

The diagram shows a "Container Storage" setup. A blue cloud icon with an upward arrow is labeled "Azure Container Instances". Below it, a dashed-line box represents a container instance. Inside this box, there is a single blue cube icon. A green curved arrow originates from this cube and points to a "Azure Files" icon at the bottom, which consists of a blue file folder and a computer monitor icon.

Container Storage

Can use Azure file shares for persistent data storage.

Container Networking

Can deploy containers as either private or public resources.



S queremos desplegar un grupo de containers se hace mediante un json

**Scaling/Sizing**

No autoscaling options available, manual redeployment of a container group is required. You determine CPU, memory, and GPU.

**Container Groups**

A top-level resource in ACI. A collection of containers that are on the same host machine and share a lifecycle and resources.

**Networking**

A container group shares an IP address and fully qualified domain name (FQDN). Ports must be opened for external access. Localhost connectivity by default within the group. Can deploy as public, private, or none.

**Storage**

Persistent storage is available by mounting a storage volume. For example, an Azure file share in Azure Files.

**Restart Policy**

Restart of containers is available using policies: Always, Never, and OnFailure.

**Environment Variables**

Save plaintext and secure environment variables to be used by a container. For example, a database connection string.

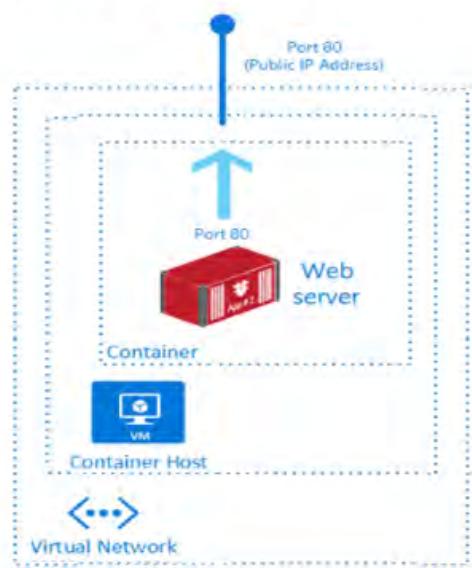
Review Azure Container Instances

✓ 100 XP

2 minutes

Containers are becoming the preferred way to package, deploy, and manage cloud applications. Azure Container Instances offers the fastest and simplest way to run a container in Azure, without having to manage any virtual machines and without having to adopt a higher-level service. Azure Container Instances is a great solution for any scenario that can operate in isolated containers, including simple applications, task automation, and build jobs.

The following illustration shows a web server container built with Azure Container Instances. The container is running on a virtual machine in a virtual network.



Things to know about Azure Container Instances

Let's review some of the benefits of using Azure Container Instances. As you review these points, think about how you can implement Container Instances for your internal applications.

- **Fast startup times.** Containers can start in seconds without the need to provision and manage virtual machines.
- **Public IP connectivity and DNS names.** Containers can be directly exposed to the internet with an IP address and FQDN (fully qualified domain name).
- **Custom sizes.** Container nodes can be scaled dynamically to match actual resource demands for an application.
- **Persistent storage.** Containers support direct mounting of Azure Files file shares.
- **Linux and Windows containers.** Container Instances can schedule both Windows and Linux containers. Specify the operating system type when you create your container groups.
- **Coscheduled groups.** Container Instances supports scheduling of multi-container groups that share host machine resources.
- **Virtual network deployment.** Container Instances can be deployed into an Azure virtual network.

Implement container groups

✓ 100 XP

3 minutes

The top-level resource in Azure Container Instances is the container group. A container group is a collection of containers that get scheduled on the same host machine. The containers in a container group share a lifecycle, resources, local network, and storage volumes.

Things to know about container groups

Things to know about container groups

Let's review some of details about container groups for Azure Container Instances.

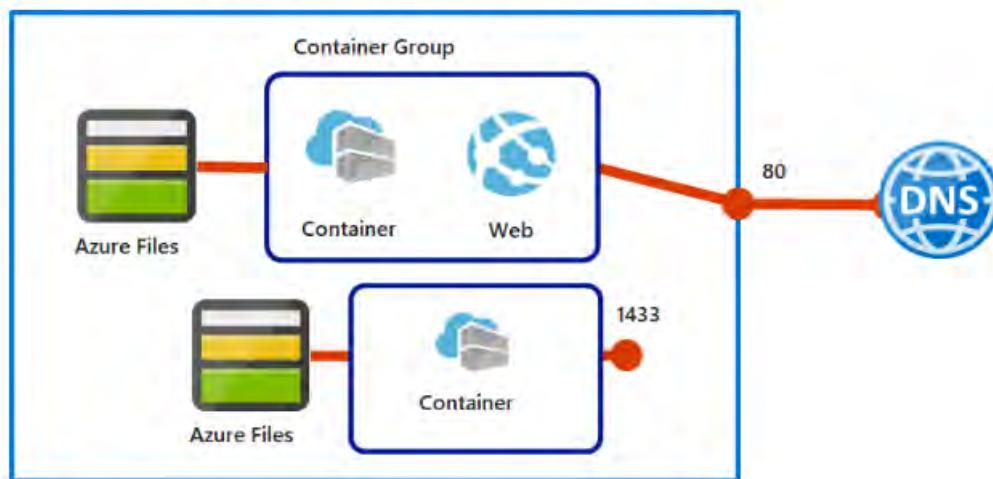
- A container group is similar to a pod in Kubernetes. A pod typically has a 1:1 mapping with a container, but a pod can contain multiple containers. The containers in a multi-container pod can share related resources.
- Azure Container Instances allocates resources to a multi-container group by adding together the resource requests of all containers in the group. Resources can include items such as CPUs, memory, and GPUs.

Consider a container group that has two containers that each require CPU resources. Each container requests one CPU. Azure Container Instances allocates two CPUs for the container group.

- There are two common ways to deploy a multi-container group: Azure Resource Manager (ARM) templates and YAML files.
 - ARM template. An ARM template is recommended for deploying other Azure service resources when you deploy your container instances, such as an Azure Files file share.
 - YAML file. Due to the concise nature of the YAML format, a YAML file is recommended when your deployment includes only container instances.
- Container groups can share an external-facing IP address, one or more ports on the IP address, and a DNS label with an FQDN.
 - External client access. You must expose the port on the IP address and from the container to enable external clients to reach a container in your group.
 - Port mapping. Port mapping isn't supported because containers in a group share a port namespace.
 - Deleted groups. When a container group is deleted, its IP address and FQDN are released.

Configuration example

Consider the following example of a multi-container group with two containers.



The multi-container group has the following characteristics and configuration:

- The container group is scheduled on a single host machine, and is assigned a DNS name label.
- The container group exposes a single public IP address with one exposed port.
- One container in the group listens on port 80. The other container listens on port 1433.
- The group includes two Azure Files file shares as volume mounts. Each container in the group mounts one of the file shares locally.

Things to consider when using container groups

Multi-container groups are useful when you want to divide a single functional task into a few container images. The images can be delivered by different teams and have separate resource requirements.

Consider the following scenarios for working with multi-container groups. Think about what options can support your internal apps for the online retailer.

- Consider web app updates. Support updates to your web apps by implementing a multi-container group. One container in the group serves the web app and another container pulls the latest content from source control.
- Consider log data collection. Use a multi-container group to capture logging and metrics data about your app. Your application container outputs logs and metrics. A logging container collects the output data and writes the data to long-term storage.
- Consider app monitoring. Enable monitoring for your app with a multi-container group. A monitoring container periodically makes a request to your application container to ensure your app is running and responding correctly. The monitoring container raises an alert if it identifies possible issues with your app.
- Consider front-end and back-end support. Create a multi-container group to hold your front-end container and back-end container. The front-end container can serve a web app. The back-end container can run a service to retrieve data.

Review the Docker platform

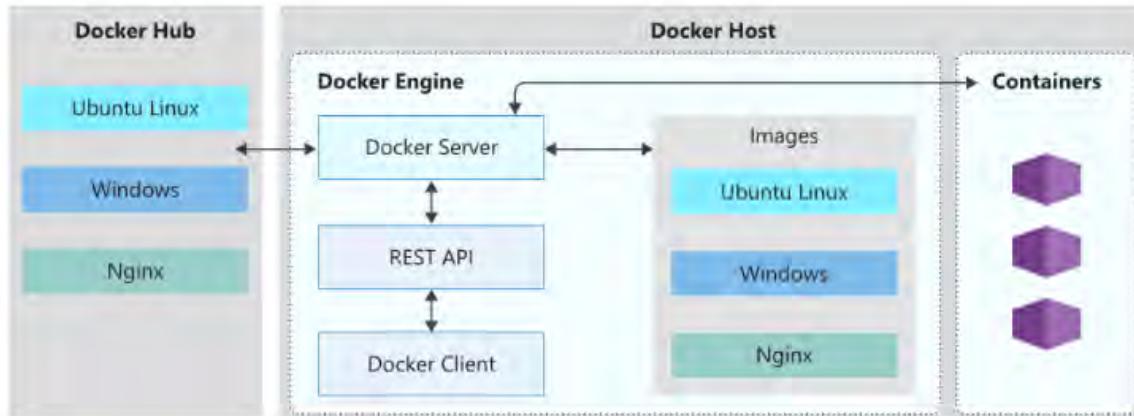
✓ 100 XP

3 minutes

Docker is a platform that enables developers to host applications within a container. A container in Docker is essentially a standalone package that contains everything needed to execute a piece of software.

Docker Hub provides a large global repository of container images from developers, open source projects, and independent software vendors. You can access Docker Hub to find and share container images for your app and containers. Docker Hosts are machines that run Docker and allow you to run your apps as containers.

The following illustration shows how Docker Hub communicates with Docker Host.



Things to know about Docker and containers

Examine the following characteristics of the Docker platform and containers.

- The Docker platform is available on both Linux and Windows and can be hosted on Azure.
- A Docker container package includes the application executable code, the runtime environment such as .NET Core, system tools, and settings.
- A Dockerfile is a text file with instructions on how to build a Docker image. The Dockerfile is like a batch script. The first line identifies the base image. The rest of the file includes the build actions.
- The key feature of Docker is the guarantee that containerized software always runs the same locally on Windows or Linux, or in the cloud on Azure.
- Develop your code locally within a Docker container, share your code with Quality Assurance resources for testing, and deploy your code to production in the Azure cloud. After your code is deployed, your app can easily be scaled by using Azure Container Instances.

Things to consider when using Docker

Before you begin using Docker and Azure Container Instances to create, build, and test containers, it's helpful to be familiar with the terminology and concepts.

- **Container:** An instance of a Docker image. A container represents the execution of a single application, process, or service. It consists of the contents of a Docker image, an execution environment, and a standard set of instructions. When scaling a service, you create multiple instances of a container from the same image. A batch job can create multiple containers from the same image, and pass different parameters to each instance.
 - **Container image:** A package with all the dependencies and information required to create a container. The dependencies include frameworks and the deployment and execution configuration that a container runtime uses. Usually, an image derives from multiple base images that are layers stacked on top of each other to form the container's file system. An image is immutable after it's created.
 - **Build:** The process of creating a container image based on the information and context provided by the Dockerfile. The build also includes any other necessary files. You build images by using the Docker `docker build` command.
 - **Pull:** The process of downloading a Docker container image from a container registry.
 - **Push:** The process of uploading a Docker container image to a container registry.
-

1. Why should you select virtual machines over containers for your configuration? *

- Virtual machines run the user mode portion of an operating system and can be tailored to contain just the needed services for your app.
- Virtual machines provide complete isolation from the host operating system and other virtual machines.
✓ Correct. Azure containers only provide lightweight isolation from the host.
- Virtual machines use Azure Disks for local storage for a single node.

2. Which of the following options is a feature of Azure Container Instances? *

- Container Instances require several minutes to load.
- Container Instances use Azure Blob Storage for retrieve and persist state.
- Billing for Container Instances occurs when containers are in use.

✓ Correct. Organizations are only billed when their Container Instances are in use.

3. What implementation ensures container software runs the same locally and in the cloud on Azure? *

- Docker
✓ Correct. Docker guarantees that containerized software always runs the same locally on Windows or Linux, and in the cloud on Azure.
- Container groups
- Container Instances

✗ Incorrect. Azure Container Instances doesn't guarantee that containerized software always runs the same.

Kubernetes Container Solution



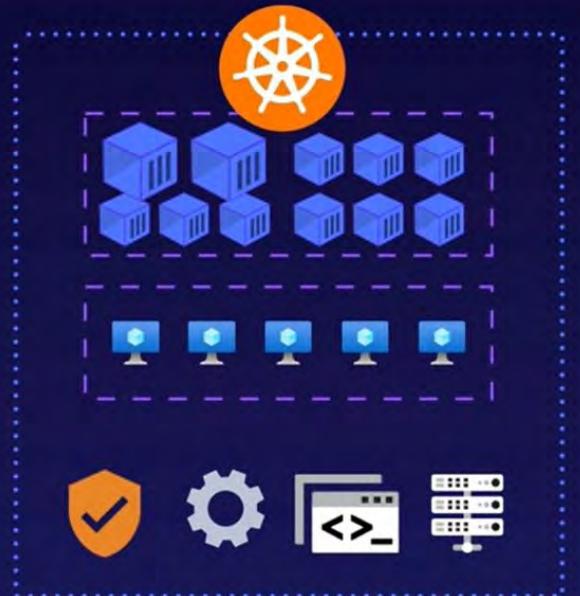
Kubernetes Benefits

Scalability

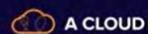
Can easily scale containers to meet demand.

Management

Provides an orchestration layer for clusters.



What Is Azure Kubernetes Service (AKS)?



AKS

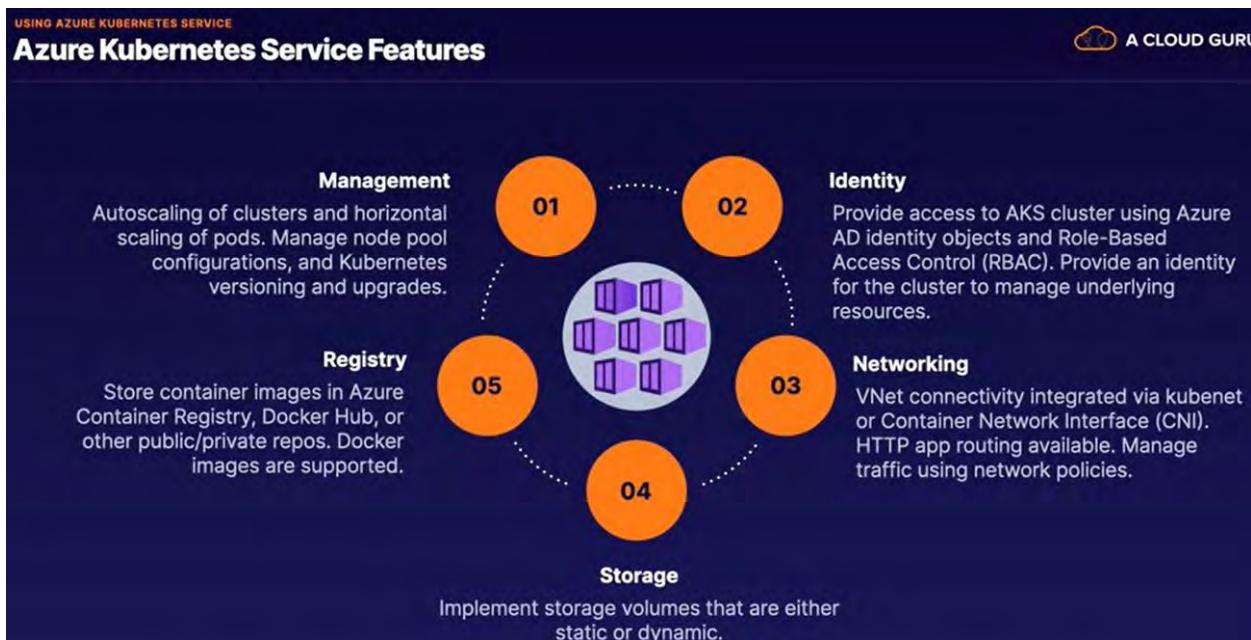
What is it?

Azure Kubernetes Service (AKS) is a serverless platform for Kubernetes. It provides scalable container solutions.

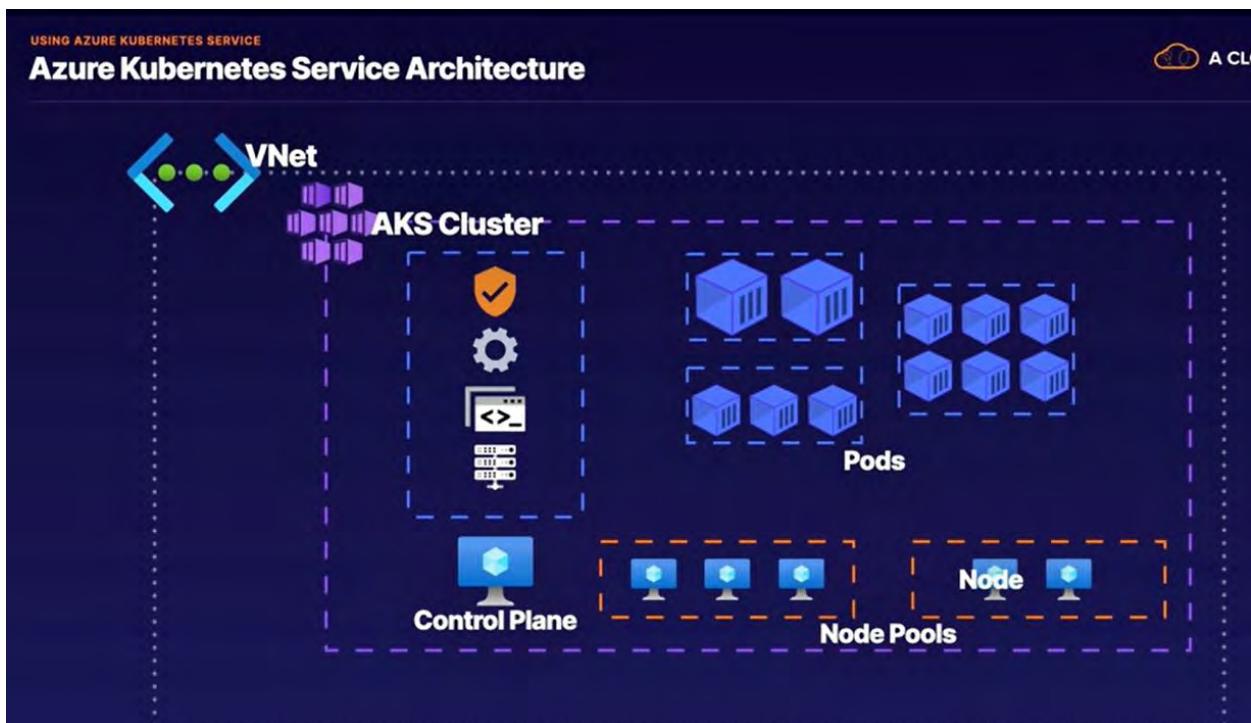
Why use it?

AKS abstracts away the management of a Kubernetes cluster by managing most of the deployment and orchestration.

	Kubernetes	AKS
Autoscaling Pods and Clusters		
Identity and Access Management Azure AD Integration		
Storage Volumes Azure Storage		
Networking VNets, NSGs, and network policies		



Arquitectura de AKS



En el control plane esta el master node que es el que orquesta todo

Loa node pools es donde los containers van a estar corriendo

Los container van dentro de los pods

Si usamos kubenet para networking hará nat de los node pools a los containers y si usamos CNI le dará una nic a cada container

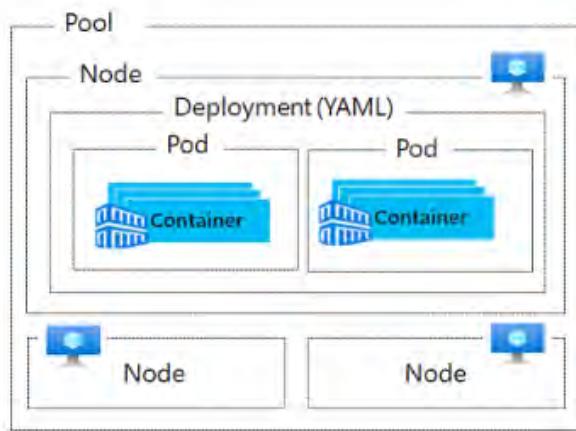
Explore Azure Kubernetes Service terminology

✓ 100 XP

2 minutes

Azure Kubernetes Service (AKS) provides a simplified approach for deploying a managed Kubernetes cluster in Azure. Azure operates as a hosted Kubernetes service and performs critical functions like health monitoring and maintenance. AKS employs components like nodes, pods, and pools to help you deploy and manage your container applications in Kubernetes clusters.

The following illustration shows the relationships in a Kubernetes pool between nodes, pods, and containers.



Things to know about AKS concepts

Before you begin using Kubernetes and Azure Kubernetes Service to deploy and manage containerized applications, it's helpful to be familiar with the terminology and concepts.

- **Pools:** A pool is a group of nodes that have an identical configuration.
- **Nodes:** A node is an individual virtual machine that runs containerized applications.
- **Pods:** A pod is a single instance of an application. A pod can contain multiple containers.
- **Container:** A container is a lightweight and portable executable image that contains software and all of its dependencies.
- **Deployment:** A deployment has one or more identical pods managed by Kubernetes.
- **Manifest:** The manifest is the YAML file that describes a deployment.

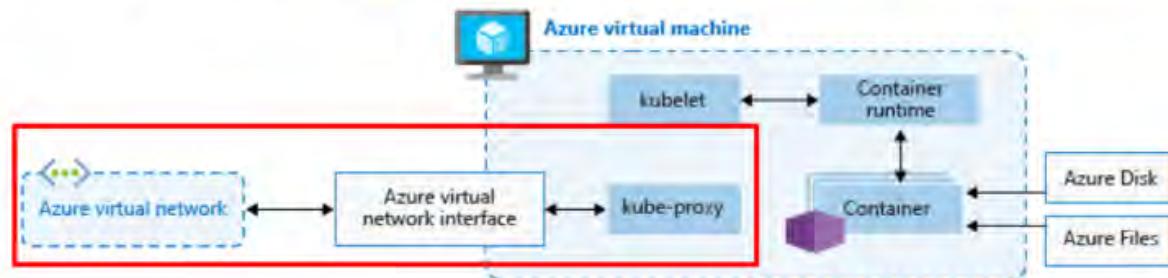
Explore the AKS cluster and node architecture

✓ 100 XP

2 minutes

An Azure Kubernetes Service cluster is divided into two components: Azure-managed nodes and customer-managed nodes. Azure-managed nodes provide the core Kubernetes services and orchestration of application workloads in your AKS cluster. Customer-managed nodes run your application workloads in your AKS cluster.

The following illustration shows an example AKS cluster. The Azure-managed node has a scheduler, controller, API server, and storage. The customer-managed node has a container runtime, kubelet agent, and kube-proxy component. We'll examine these items in the following section.



Things to know about AKS clusters, nodes, and pools

Let's take a closer look at how Azure Kubernetes Service implements clusters and nodes.

- To run your applications and supporting services, you need a Kubernetes node for your AKS cluster. Each AKS cluster contains one or more nodes that run the Kubernetes node components and the container runtime.
- Nodes are instances of Azure Virtual Machines. Nodes of the same configuration are grouped together into node pools. A Kubernetes cluster contains one or more node pools.
- The initial number of nodes and size are defined when you create an AKS cluster, which creates the default node pool. The default node pool in AKS contains the underlying virtual machines that run your agent nodes.
- When you create an AKS cluster, an Azure-managed cluster node is automatically created and configured. This node is provided as a managed Azure resource that's abstracted from the user.
- The kubelet is the Kubernetes agent that processes the orchestration requests from the Azure-managed node, and scheduling of running the requested containers.
- The kube-proxy component handles virtual networking on each node. The proxy routes network traffic and manages IP addressing for services and pods.
- The container runtime component allows containerized applications to run and interact with other resources such as the virtual network and storage.
 - AKS clusters with Kubernetes version 1.19 node pools and later use containerd as the container runtime.
 - AKS clusters with node pools that use Kubernetes versions earlier than v1.19 implement Moby (upstream Docker) as the container runtime.
- When you implement Azure Kubernetes Service clusters, you pay only for running agent nodes in your cluster.

Configure Azure Kubernetes Service networking

100 XP

3 minutes

Kubernetes provides an abstraction layer for virtual networking to allow access to your applications, or for application components to communicate with each other. Kubernetes uses pods to run an instance of your application, and provides different services to logically group pods. This arrangement allows for direct access via an IP address or domain name system (DNS) name and on a specific port. Azure Kubernetes Service expands on the Kubernetes features to simplify the process to support networking.

Things to know about Kubernetes virtual networking

Let's review how virtual networking is supported in Kubernetes.

- Kubernetes nodes are connected to a virtual network, which provides inbound and outbound connectivity for pods.
- The kube-proxy component runs on each node to provide the network features.
- Network policies configure security and filtering of the network traffic for pods.
- Network traffic can be distributed by using a load balancer.
- Complex routing of application traffic can be achieved with Ingress Controllers.

Azure Kubernetes Service

The Azure platform helps to simplify virtual networking for Azure Kubernetes Service clusters.

When you create a Kubernetes load balancer, the underlying Azure Load Balancer resource is created and configured. As you open network ports to pods, the corresponding Azure network security group rules are configured. For HTTP application routing, Azure can configure an external DNS as new ingress routes are configured.

Things to know about Kubernetes service types

To simplify the network configuration for application workloads, Kubernetes uses services to logically group a set of pods together and provide network connectivity. There are four service types available for creating network configurations.

Service type	Description	Scenario
Cluster IP	Create an internal IP address for use within an Azure Kubernetes Service cluster.	Implement internal-only applications that support other workloads within the cluster
NodePort	Create a port mapping on the underlying node.	Allow direct access to the application with the node IP address and port
LoadBalancer	Create an Azure Load Balancer resource, configure an external IP address, and connect the requested pods to the load balancer back-end pool.	Allow customer traffic to reach the application by creating load-balancing rules on the desired ports
ExternalName	Create a specific DNS entry.	Support easier application access

Here are some details about these network configuration options:

- You can create internal and external load balancers.
- The IP address for load balancers and services can be dynamically assigned, or you can specify an existing static IP address.
- Internal load balancers are only assigned a private IP address, so can't be accessed from the internet.
- Both internal and external static IP addresses can be assigned. The existing static IP address is often tied to a DNS entry.

Things to know about Kubernetes pods

Kubernetes uses pods to run an instance of your application, where a pod represents a single instance of your application.

Let's examine how Kubernetes uses pods and containers to support networking.

- Pods typically have a 1:1 mapping with a container, although there are advanced scenarios where a pod might contain multiple containers.
- Multi-container pods are scheduled together on the same node, and allow containers to share related resources.
- When you create a pod, you can define resource limits to request a certain amount of CPU or memory resources. The Kubernetes Scheduler attempts to schedule the pods to run on a node with available resources to meet the request.
- You can specify maximum resource limits that prevent a given pod from consuming too much compute resource from the underlying node.

ⓘ Note

A best practice is to include resource limits for all pods to help the Kubernetes Scheduler recognize what resources are needed and permitted.

- A pod is a logical resource, but a container is where the application workloads run.

Pods are typically ephemeral, disposable resources. Individually scheduled pods miss some of the high availability and redundancy features Kubernetes provides. Instead, pods are commonly deployed and managed by Kubernetes controllers, such as the Deployment controller.

Configure Azure Kubernetes Service storage

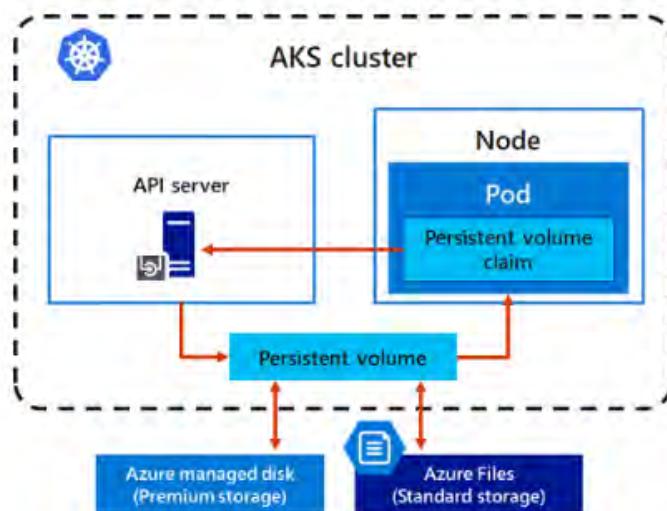
100 XP

5 minutes

There are different scenarios where applications in an Azure Kubernetes Service cluster might need to store and retrieve data. Consider the following examples:

- Your application workload uses local, fast data storage on a node that's not needed after the pods are deleted.
- Your application workload requires storage that persists on more regular data volumes within the Azure platform.
- Multiple pods share the same data volumes, or reattach data volumes if the pod is rescheduled on a different node.
- You need to inject sensitive data or application configuration information into pods.

The following illustration highlights storage options for applications in an AKS cluster.



Let's examine four core concepts about providing storage for your applications in AKS: storage volumes, persistent volumes, storage classes, and volume claims.

Things to know about storage volumes

Applications often need to store and retrieve data. Because Kubernetes typically treats individual pods as ephemeral, disposable resources, different approaches are available for applications to use and persist data as necessary. Storage volumes represent a way to store, retrieve, and persist data across pods and through the application lifecycle.

- Traditional storage volumes that store and retrieve data are created as Kubernetes resources backed by Azure Storage.
- You can manually create storage volumes to be assigned to pods directly, or have Kubernetes automatically create them.
- Storage volumes can use Azure Disks or Azure Files:
 - Use Azure Disks to create a Kubernetes *DataDisk* resource. Disks can use Azure Premium storage, backed by high-performance SSDs, or Azure Standard storage, backed by regular HDDs. For most production and development workloads, use Premium storage. Azure Disks are mounted with *ReadWriteOnce* permissions, so they're available to a single node only. For storage volumes that can be accessed by multiple nodes simultaneously, use Azure Files.
 - Use Azure Files to mount an SMB 3.0 share backed by an Azure storage account to pods. Azure Files let you share data across multiple nodes and pods. Files can use Azure Standard storage backed by regular HDDs, or Azure Premium storage, backed by high-performance SSDs.

Things to know about persistent volumes

Volumes are defined and created as part of the pod lifecycle and exist only until the pod is deleted. Pods often expect their storage to remain if a pod is rescheduled on a different host during a maintenance event, especially in `statefulsets` configurations. A persistent volume (`PersistentVolume`) is a storage resource that's created and managed by the Kubernetes API that can exist beyond the lifetime of an individual pod.

- You can use Azure Disks or Azure Files to provide a persistent volume. The choice of whether to use Azure Disks or Azure Files is often determined by the need for concurrent access to the data or the performance tier.
- A persistent volume can be statically created by a cluster administrator, or dynamically created by the Kubernetes API server.
- If a pod is scheduled, and requests Storage that's not currently available, Kubernetes can create the underlying Azure Disks or Azure Files storage. Kubernetes also attaches the storage volume to the pod.
- Dynamic provisioning uses a `StorageClass` type to identify what kind of Azure Storage needs to be created.

Things to know about storage classes

To define different tiers of storage, such as Premium and Standard, you can configure a `storageClass` type. The `StorageClass` type also defines the `reclaimPolicy` actions for the storage. The `reclaimPolicy` definition controls the behavior of the underlying Azure Storage resource when the pod is deleted and the persistent volume might no longer be required. The underlying Storage resource can be deleted, or retained for use with a future pod.

In Azure Kubernetes Service, four initial `storageClasses` types are created for a cluster by using in-tree storage plugins:

StorageClass type	Description	reclaimPolicy action
<code>default</code>	Use Azure StandardSSD storage to create an Azure managed disk.	Ensures the underlying Azure disk is deleted when the persistent volume that used the disk is deleted.
<code>managed-premium</code>	Use Azure Premium storage to create an Azure managed disk.	Ensures the underlying Azure disk is deleted when the persistent volume that used the disk is deleted.
<code>azurefile</code>	Use Azure Standard storage to create an Azures Files file share.	Ensures the underlying Azure Files file share is deleted when the persistent volume that used the file share is deleted.
<code>azurefile-premium</code>	Use Azure Premium storage to create an Azures Files file share.	Ensures the underlying Azure Files file share is deleted when the persistent volume that used the file share is deleted.

If no `storageClass` type is specified for a persistent volume, the `default` type is used.

Important

Take care when requesting persistent volumes, and ensure your volumes use the storage you require. You can create a `StorageClass` type to satisfy subsequent requirements by using the Azure CLI `kubectl` tool.

Things to know about persistent volume claims

A persistent volume claim (`PersistentvolumeClaim`) requests either Azure Disks or Azure Files storage of a particular `StorageClass`, access mode, and size.

- The Kubernetes API server can dynamically provision the underlying storage resource in Azure, if there's no existing resource to fulfill the claim based on the defined `storageClass` type.
- The pod definition includes the volume mount after the volume has been connected to the pod.
- A persistent volume is *bound* to a persistent volume claim after an available Storage resource is assigned to the pod that requests the volume.
- There's a 1:1 mapping of persistent volumes to claims.

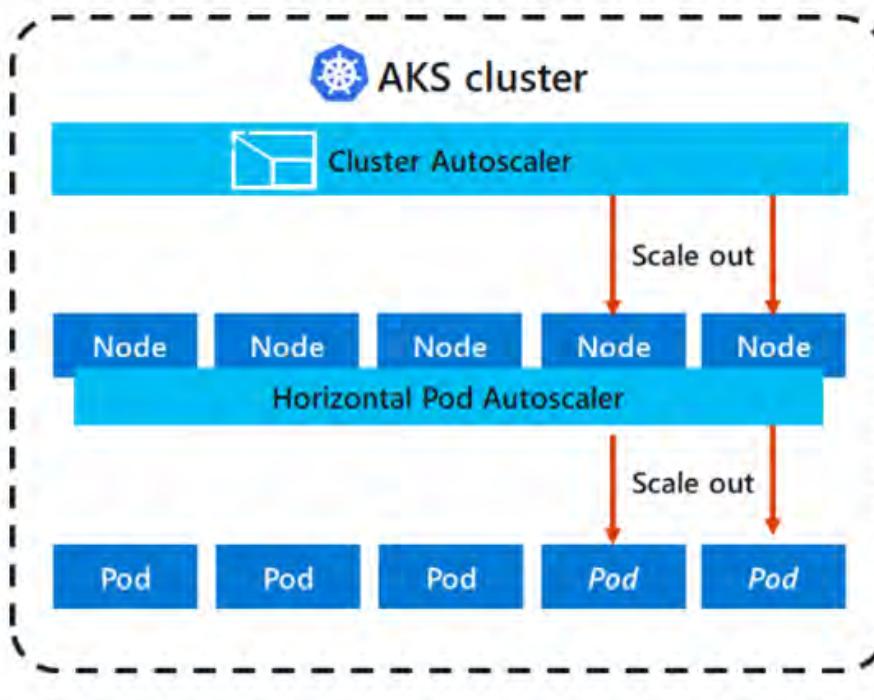
Configure Azure Kubernetes Service scaling

100 XP

5 minutes

The process of scaling involves adjusting the compute resources allocated for your application instances to meet workload demands. When you run applications in an Azure Kubernetes Service cluster, you might need to apply scaling to increase or decrease your compute resources. If the number of your application instances changes, the number of underlying Kubernetes nodes might also need to change. You might also need to quickly provision a large number of extra application instances.

The following illustration shows a scaling implementation for Azure Kubernetes Service.



Things to know about scaling techniques

In an Azure Kubernetes Service cluster, you can manually scale pods or nodes, and automatically scale pods or clusters.

Scaling technique	Description	Version requirements
Manually scale pods or nodes	Manually scale your replicas (pods) and nodes to test how your application responds to changes in available resources and state. Manually scaling resources lets you define a specific number of resources to use to maintain a fixed cost, such as the number of nodes. To manually scale, you define the replica or node count, and the Kubernetes API schedules creating new pods or draining nodes.	All Kubernetes versions
Automatically scale pods	Use the horizontal pod autoscaler (HPA) to monitor resource demand and automatically scale the number of your replicas. By default, the HPA checks the Metrics API every 30 seconds for any required changes in your replica count. When changes are required, the number of replicas is increased or decreased accordingly.	AKS clusters that deploy the Metrics Server for Kubernetes 1.8 or later
Automatically scale clusters	Respond to changing pod demands with the cluster autoscaler, which adjusts the number of your nodes based on the requested compute resources in the node pool. By default, the cluster autoscaler checks the API server every 10 seconds for any required changes in the node count. If the cluster autoscale determines a change is required, the number of nodes in your AKS cluster is increased or decreased accordingly.	RBAC-enabled AKS clusters that run Kubernetes 1.10.x or later

Things to consider when using horizontal autoscaling

Let's review some details about working with the horizontal pod autoscaler.

- Consider number of pods (replicas). When you configure the HPA for a given deployment, you define the minimum and maximum number of pods (replicas) that can run.
- Consider scaling metrics. To use the HPA, define the metric to monitor and to use as the basis for scaling decisions, such as CPU usage.
- Consider cooldown for scaling events. As the HPA checks the Metrics API every 30 seconds, previous scale events might not complete before subsequent checks occur. The HPA might change the number of replicas before the previous scale event receives the application workload and resource demands to adjust accordingly.

To minimize race events, set cooldown or delay values to define how long the HPA must wait after a scale event before another scale event is triggered. This behavior allows the new replica count to take effect and the Metrics API to reflect the distributed workload. By default, the delay on scale up events is 3 minutes, and the delay on scale down events is 5 minutes.

- Consider tuning cooldown values. You might need to tune cooldown values. Default cooldown values might give the impression that the HPA isn't scaling the replica count quickly enough. To more quickly increase the number of replicas in use, reduce the `--horizontal-pod-autoscaler-upscale-delay` value when you create your HPA definitions by using the Azure CLI `kubectl` tool.

Things to consider when using cluster autoscaling

Now let's consider the details for working with the cluster autoscaler.

- Consider combining with HPA. Cluster autoscaler is typically used alongside the horizontal pod autoscaler. When the two scaling techniques are combined, the HPA increases or decreases the number of pods based on application demand. The cluster autoscaler adjusts the number of nodes as needed to run the extra pods accordingly.
- Consider scale-out events. If a node doesn't have sufficient compute resources to run a requested pod, that pod can't progress through the scheduling process. The pod can't start unless other compute resources are available within the node pool.

When the cluster autoscaler notices pods that can't be scheduled due to node pool resource constraints, the number of nodes within the node pool is increased to provide the extra compute resources. When the extra nodes are successfully deployed and available for use within the node pool, the pods are then scheduled to run on them.

- Consider burst scaling to Azure Container Instances. If your application needs to scale rapidly, some pods might remain in a state waiting to be scheduled until the new nodes deployed by the cluster autoscaler can accept the scheduled pods. For applications that have high burst demands, you can scale with virtual nodes and Azure Container Instances. We take a closer look at rapid burst scaling in the next section.
- Consider scale-in events. The cluster autoscaler monitors the pod scheduling status for nodes that haven't recently received new scheduling requests. This scenario indicates that the node pool has more compute resources than required, so the number of nodes can be decreased.

A node that passes a threshold for not being needed for 10 minutes is scheduled for deletion by default. When this situation occurs, pods are scheduled to run on other nodes within the node pool, and the cluster autoscaler decreases the number of nodes.

- Consider avoiding single pods. Your applications might experience some disruption as pods are scheduled on different nodes when the cluster autoscaler decreases the number of nodes. To minimize disruption, avoid applications that use a single pod instance.

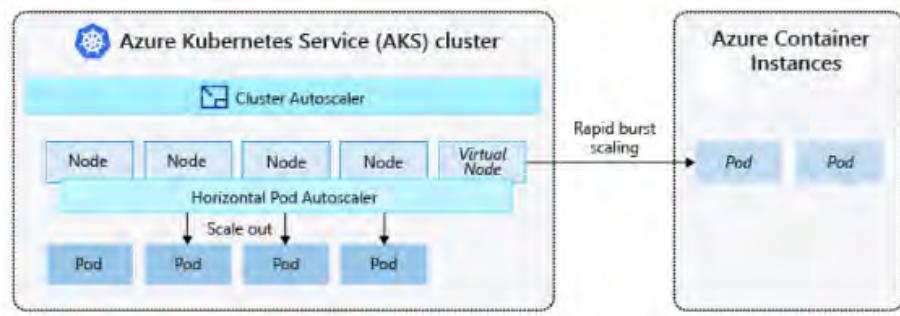
Configure AKS burst scaling to Azure Container Instances

✓ 100 XP

2 minutes

Kubernetes has built-in components to scale your replicas (pods) and nodes. If your application needs to scale rapidly, the horizontal pod autoscaler might schedule more pods than can be provided by the existing compute resources in the node pool. As a result, the cluster autoscaler is triggered to deploy more nodes in the node pool. This scenario can take a few minutes for the nodes to successfully provision.

To resolve this situation, you can rapidly scale your Azure Kubernetes Service cluster by integrating with Azure Container Instances. The following illustration shows an AKS cluster with rapid burst scaling of virtual nodes in AKS to pods in Container Instances.



Things to know about rapid burst scaling

Review the following characteristics of an AKS cluster that uses Azure Container Instances for rapid burst scaling.

- Azure Container Instances lets you quickly deploy your container instance without extra infrastructure overhead. When you connect with AKS, your container instance becomes a secured, logical extension of your AKS cluster.
- The Virtual Kubelet component is installed in your AKS cluster. The component presents your container instance as a virtual Kubernetes node.
- Kubernetes schedules pods to run as container instances through virtual nodes, rather than pods on virtual machine nodes directly in your AKS cluster.
- Your application requires no modification to use virtual nodes.
- Deployments can scale across AKS and Container Instances. There's no delay when the cluster autoscaler deploys new nodes in your AKS cluster.
- Virtual nodes are deployed to another subnet in the same virtual network as your AKS cluster. This virtual network configuration allows the traffic between Container Instances and AKS to be secured. Like an AKS cluster, a container instance is a secure, logical compute resource that's isolated from other users.

1. Which Kubernetes component processes orchestration requests and schedules when to run requested containers? *

container

kubelet

✓ Correct. The kubelet agent processes the orchestration requests from the Azure-managed node.

node

2. How does Kubernetes enable internal-only applications to support other workloads within the cluster? *

The LoadBalancer service

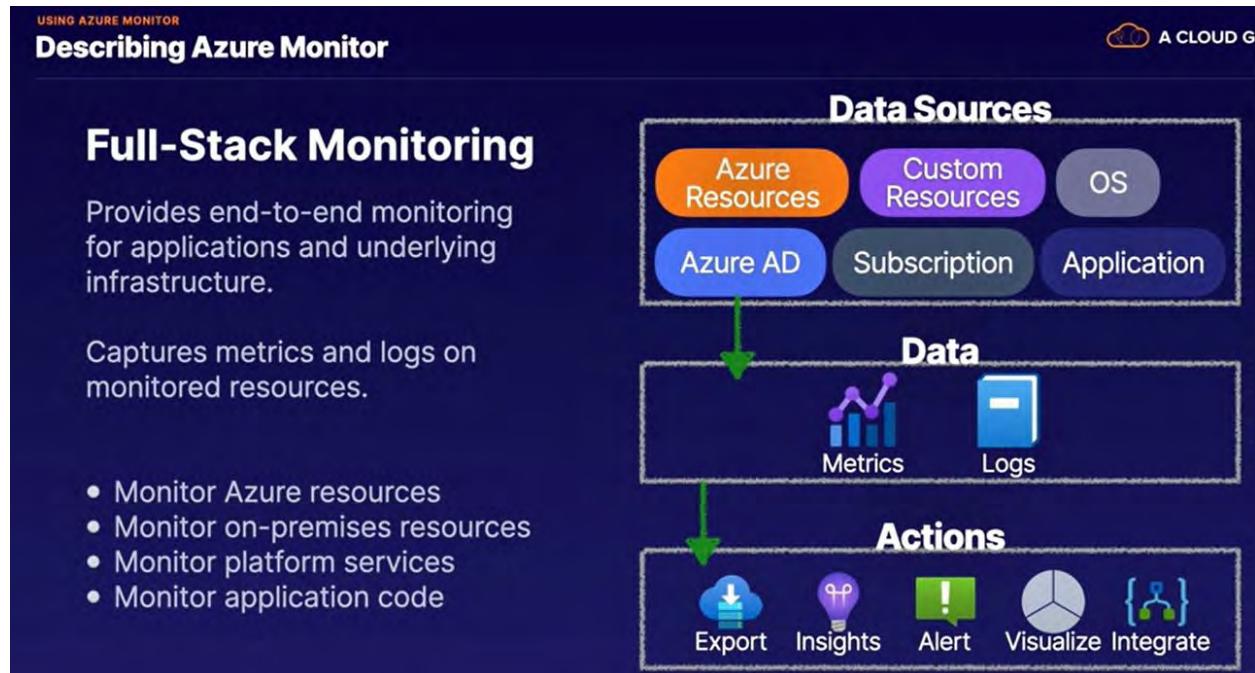
The NodePort service

✗ Incorrect. The NodePort service creates a port mapping on the underlying node that allows the application to be accessed directly with the node IP address and port.

The ClusterIP service

✓ Correct. The ClusterIP service creates an internal IP address for use within the Azure Kubernetes Service cluster.

Using Azure Monitor



Metrics vs. Logs

Metrics

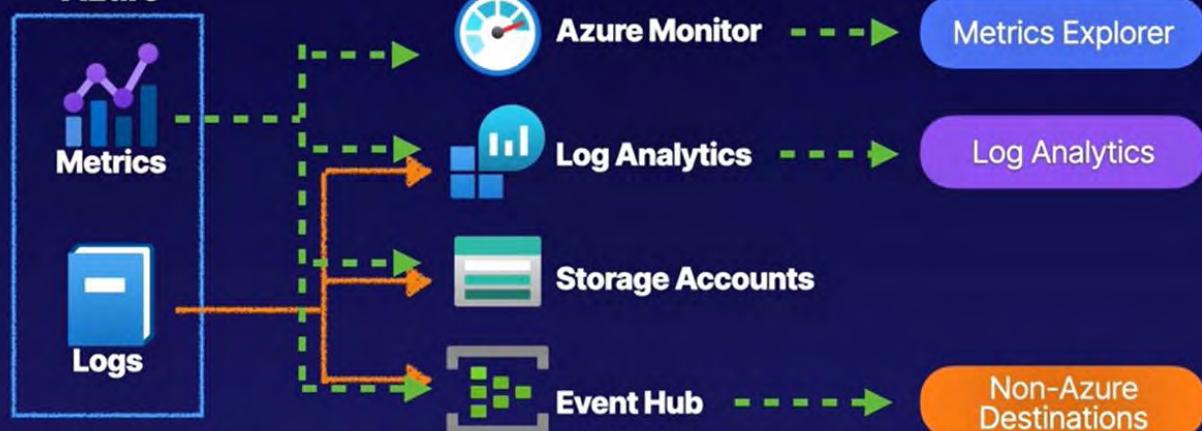
- Short, time-based data
- Frequently updated
- Near real-time data
- Alerts based on numeric values
- Visualization via Metrics Explorer

Logs

- Long, event-based data
- Sporadically updated
- Free-form and/or structured
- Stored in Log Analytics workspace
- Built-in query language (Kusto)

VS

Azure



Metrics

Metrics are gathered on a per-resource basis.

How to use metrics?

- View metrics in Metrics Explorer
- Query in Log Analytics
- Alert and take action
- Export and archive

Logs

Logs are not gathered by default by the Azure platform.

How to use logs?

- Query in Log Analytics
- Archive
- Stream to third party

Diagnostic Settings

Define how and where metrics and logs will be stored on a per-resource basis.

- OS-level data
- App-level data

Setting Up alert and actions

Describing Azure Monitor Alerts

Azure Monitor Alerting

Alerts on signals that prompt you to take proactive actions and help automate monitoring and diagnostics.

Signal Types
Metric, activity, and log signals

Action Group
The actions that will take place when an alert has been triggered

The diagram illustrates the three components of an Azure Monitor Alert:

- Resource:** Represented by a computer monitor icon.
- Condition:** Represented by two overlapping circles: one orange labeled "Signals" and one blue labeled "Logic".
- Actions:** Represented by three icons: a smartphone, an envelope, and a purple rounded rectangle labeled "Action Group".

Configuring Azure Monitor Logs

Describing Azure Monitor Logs

Azure

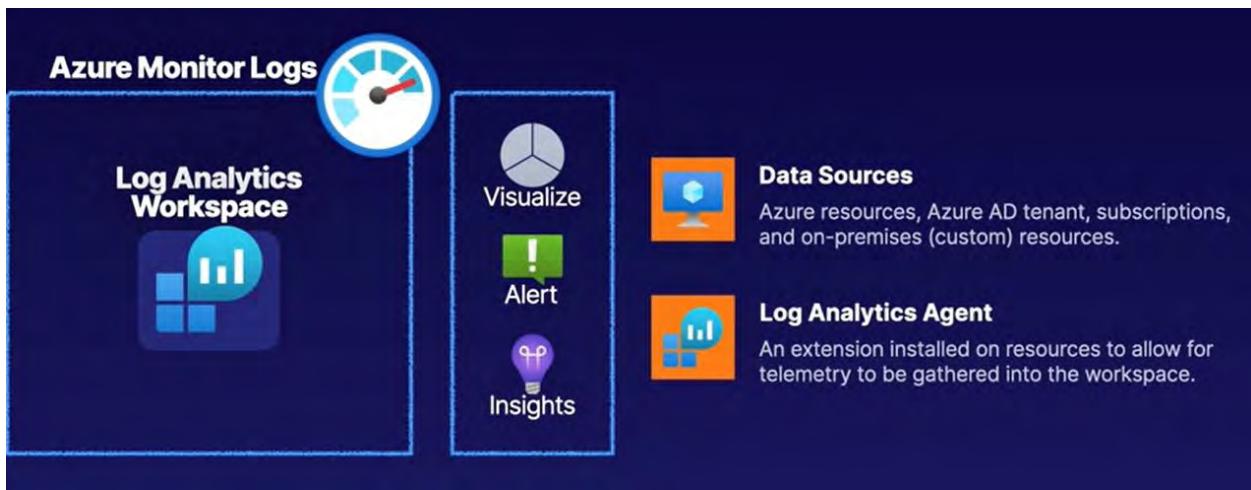
Metrics and Logs from Azure are sent to the Log Analytics Workspace.

Log Analytics

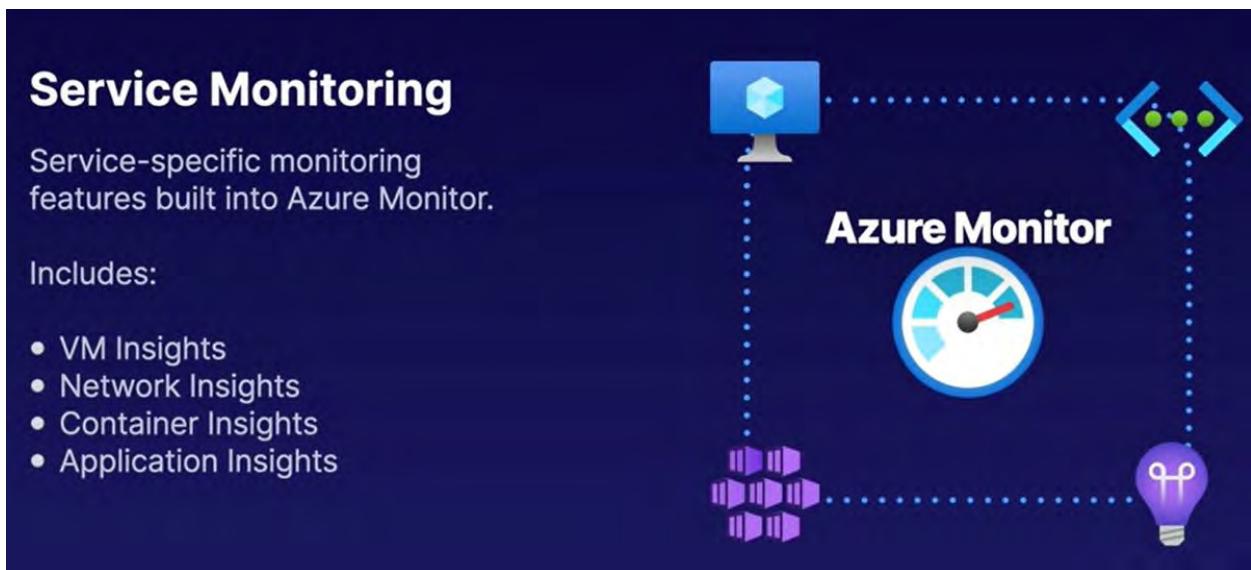
A service for aggregating log data in a single pane, where it can be analyzed, visualized, and queried.

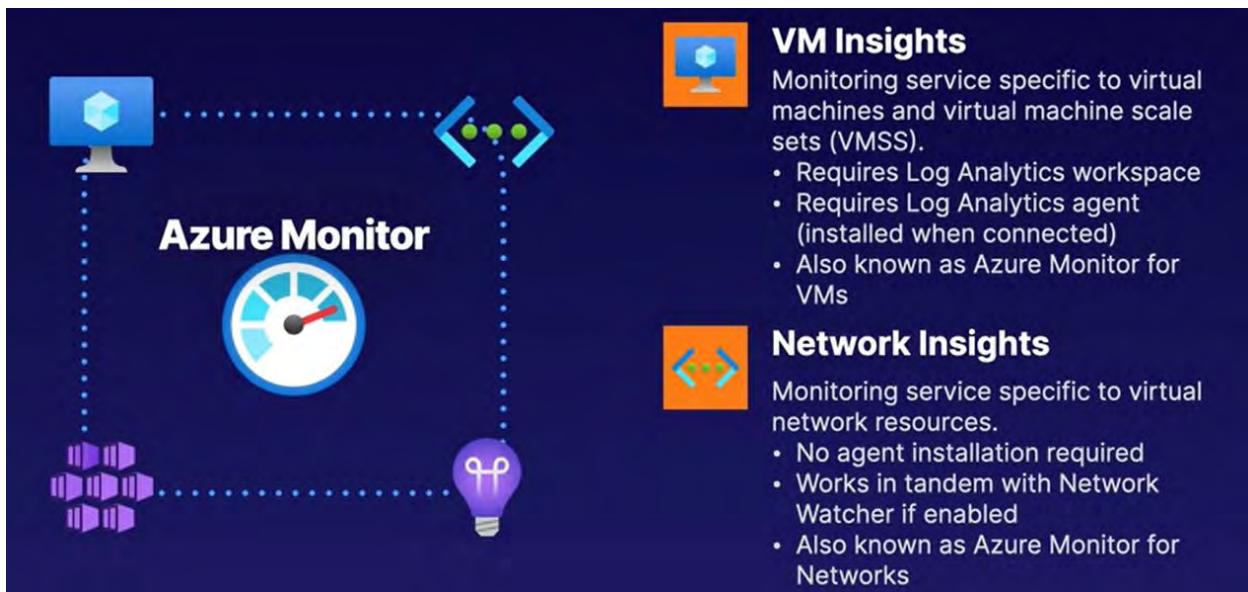
Internal Data
Azure resources, Azure AD tenant, and subscriptions

External Data
On-premises resources in hybrid environments



Understanding Monitor Insights





Configuring Application insights

Application Insights

A full-stack application monitoring solution that developers can use to monitor applications.

- Supports any application instrumented with Application Insights
- Repository for events and metrics data
- Telemetry data is streamed into an Application Insight resource



CONFIGURING APPLICATION INSIGHTS

Application Insights Features



Metrics

Live Metrics Stream for near-real-time metrics data and Metrics Explorer for viewing how metrics vary over time.

01

02

Alerts

Alerting on metrics or event data to notify application administrators of issues.

Usage Analytics

Analyze user metrics from client-side events like user interaction.

05

03

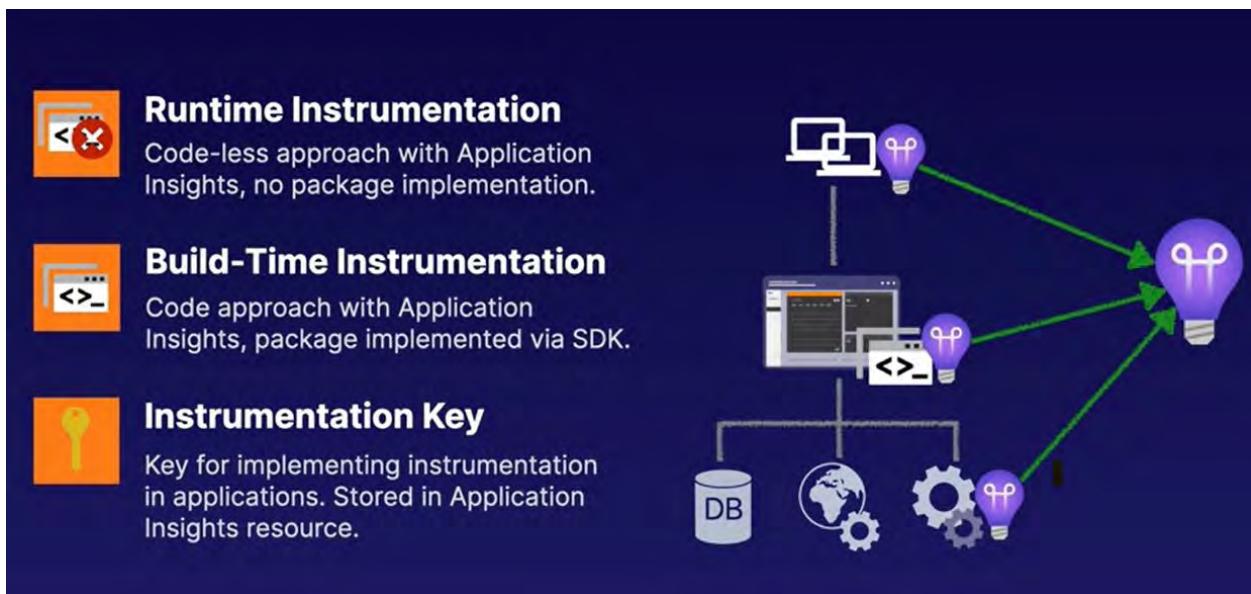
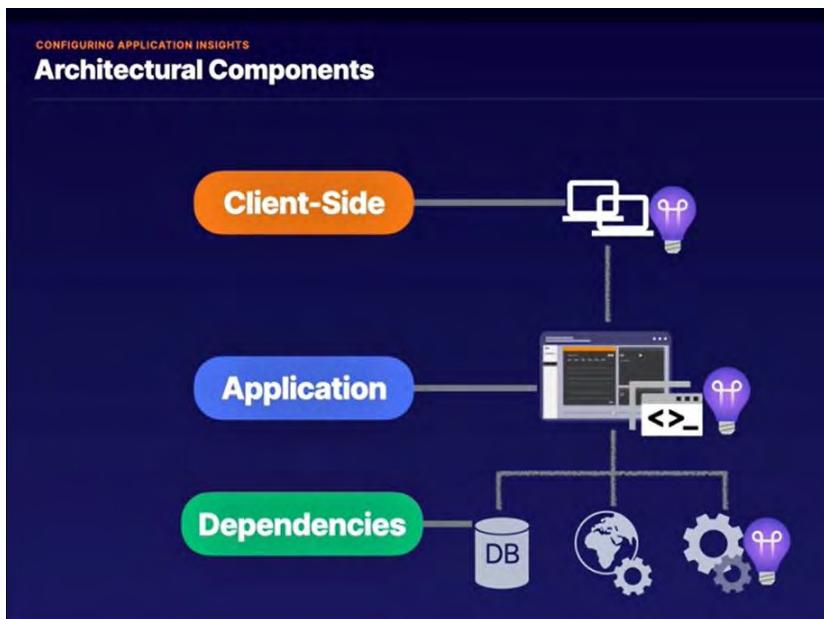
Profiler

Determine how requests are delivered, such as page elements and their performance.

Application Map

A topological view of applications and dependencies, used to identify dependency issues such as bottlenecks.

04



Using network watcher

Azure Network Watcher

Azure Network Watcher is a service comprised of networking tools for monitoring and diagnostics.

- Overview of topologies
- Monitor connectivity in Azure
- Monitor connectivity in hybrid networks
- Troubleshoot connectivity issues
- Troubleshoot hybrid network solutions
- Enable per region in a subscription



USING NETWORK WATCHER

Key Takeaways

A CLOUD GURU

Monitoring Tools



Topology

10.0.0.0

View a diagram of the resources in the virtual network



Connection Monitor

Monitor connectivity between Azure resources on the network



Network Performance Monitor

Monitor network performance and connectivity between VNets, datacenter, and/or ExpressRoute from a centralized location

Diagnostic Tools



IP Flow Verify

Test if traffic is allowed or denied inbound or outbound from VMs



Next Hop

Determine how traffic hops from VM to DEST



Effective Security Rules

Determine effective security rules on a NIC



Packet Capture

Capture packets to and/or from a VM for analysis



Connection Troubleshoot

Determine connectivity between SRC and DEST VM



VPN Diagnostics

Diagnose and troubleshoot potential VNet gateway issues

Understanding Disaster Recovery

UNDERSTANDING DISASTER RECOVERY

Describing Disaster Recovery

A CLOUD G...

What is Disaster Recovery?

The process of recovering from a disaster, such as a datacenter power outage. Every business needs a business continuity and disaster recovery (BCDR) plan.

- Assess risks
- Determine critical workloads
- Decide backup technique
- Test disaster recovery



UNDERSTANDING DISASTER RECOVERY

Recovery Point Objectives (RPO) vs. Recovery Time Objectives (RTO)

A CLOUD G...



Disaster Recovery Methods

Backup

A copy of business critical data

Cold Site

A copy of critical infrastructure that needs preparation before disaster recovery is complete

Hot Site

A copy of critical infrastructure and data that is ready to be swapped in as the production workload

Configuring Azure Backup

CONFIGURING AZURE BACKUP

Describing Azure Backup

A Cloud Guru

Backup as a Service

Azure Backup is a managed service for backing up and recovering workloads.

Requires an Azure Recovery Services vault.

Supported workloads:

- Azure virtual machines
- On-premises machines
- SQL Server workloads
- SAP HANA workloads

Components of Azure Backup

A Cloud Guru

Azure Backup

Recovery Services Vault

Workload

Start backup job

Receives backup data

1

2

3

Backup Policy

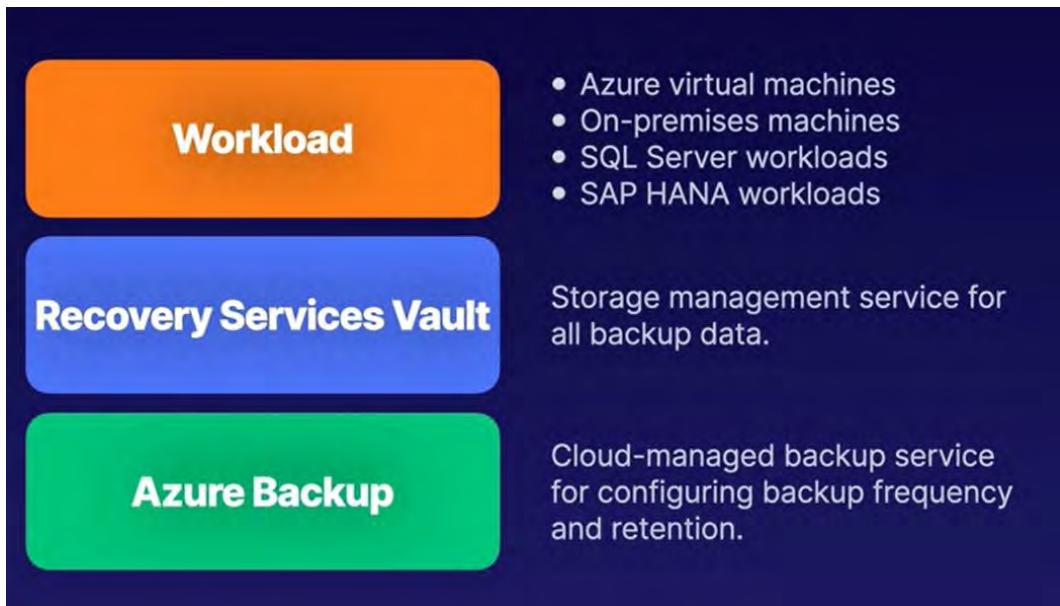
Where is your workload running?

Azure

What do you want to backup?

Virtual machine

- Virtual machine
- Azure file share
- SQL Server in Azure VM
- SAP HANA in Azure VM

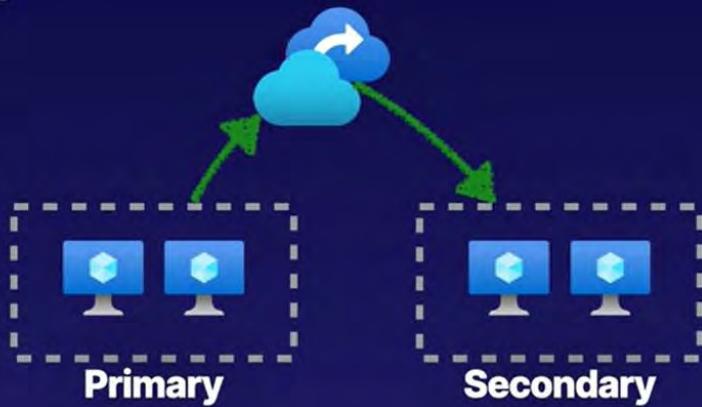


Disaster Recovery Solution

Azure Site Recovery service provides a solution for automating disaster recovery.

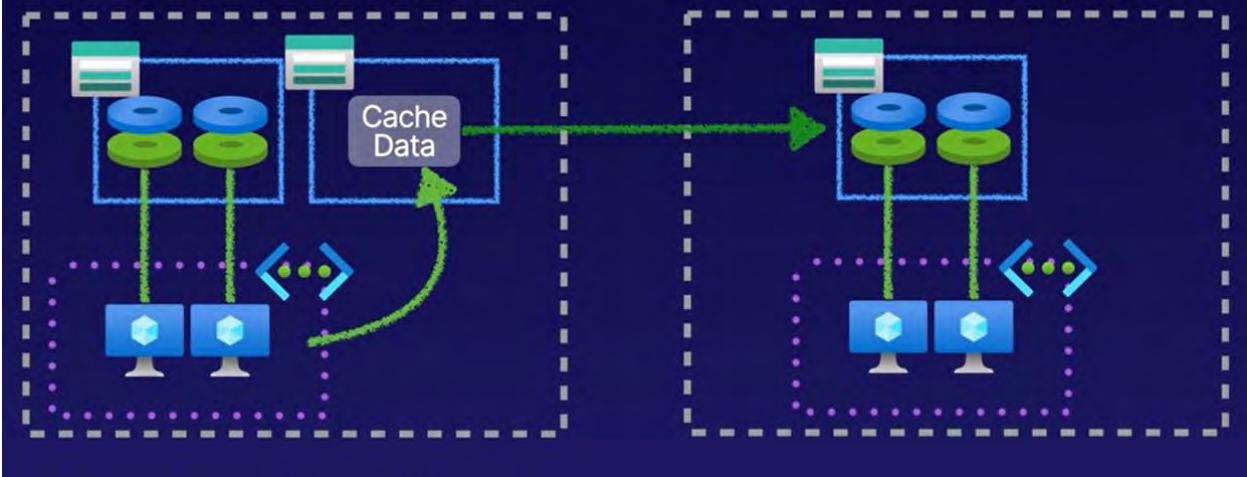
Requires an Azure Recovery Services vault.

- Cross-zone
- Cross-region



Source (East US)

Target (East US 2)



Key Takeaways

A CLOUD COMPUTING



Replicated Items

The workload that will be replicated site-to-site by Azure Site Recovery.



Replication Policy

Defines the frequency of snapshots and retention period of recovery points. Can be app-consistent or crash-consistent.



Recovery Plan

Automate and run test failover events with protected items and pre- and/or post-scripts.



Backup Reports

Backup Reports

Provides insight on backups from Azure Backup, and those insights can be used to inform items such as:

- Forecasts for cloud storage consumption
- Audits of backup and restore events

Uses Log Analytics as its logging service.



Backup Reports

- View backup policies
- View backup jobs
- View backup items
- View summary of estate



Examen

DOMAIN

Manage Azure Active Directory Identity and Governance

Active Directory (Azure AD) is Microsoft's cloud-based identity and access management service which helps users sign in and access resources in the cloud. Azure AD is intended for IT admins and app developers to control access to organizational resources and applications within. Additionally, we can use Azure AD to automate user provisioning between our existing Windows Server AD and our cloud apps, including Office 365. Finally, Azure AD gives us powerful tools to meet our governance requirements and automatically help protect user identities and credentials. Questions for this domain comprise **17% of the total questions** for the exam.

QUESTION 28

You have just created your first Azure AD tenant for our organization. You have a domain that you prefer to use over the *@example.onmicrosoft.com provided domain. You want to use the domain cloudfchase.com so that all users will have *@cloudfchase.com for their user principal naming method. How can you ensure this happens?

Verify ownership of the domain Selected

When configuring a custom domain for the Azure AD tenant, you will have to verify ownership of the domain for security purposes.

Create a record in the DNS Zone for the domain Selected

In order to configure a custom domain for an Azure AD tenant, you have to add a DNS record, such as a CNAME record, as part of setting up the custom domain.

Add a custom domain

By adding a custom domain for our Azure AD tenant, you can ensure that all users end up with the desired user principal name.

Create an Azure DNS private zone Selected

Creating an Azure DNS private zone will not help you configure a custom domain for the Azure AD tenant. Private zones are used to configure private name resolution within a network such as a VNet.

QUESTION 35

In your organization, you have a subscription with 3 resource groups. You are trying to track the costs of resources by department, but every department uses resources from each resource group. How can you best enable the organization to track the costs of its resources?

Filter cost analysis by resource groups

Assign tags to each resource group

Selected

Assigning tags to each resource group will not allow you to accurately filter down the cost of specific resources, because tags are not inherited from resource groups down to resources that they contain.

Assign tags to each resource

Assigning tags to each resource in the subscriptions allows you to filter when performing cost analysis.

Create resource locks for each resource

QUESTION 48

In regards to the governance capabilities of Azure, which of the following statements is true?

Resources inherit the tags of their resource group

Selected

Resources do not inherit tags from their resource groups. Each resource must be individually tagged.

Resource groups can be nested in one another

Resource locks are inherited from parent scopes

Resource locks are inherited from the parent scope. For example, if you lock a resource group, then all resources within that resource group are also affected by this lock.

Resources can be moved without validation

QUESTION 55

In your subscription, there are four different resource groups: RG1, RG2, RG3, and RG4. RG2 has a Read-Only lock at the resource group scope. RG3 has a Delete lock at the resource group scope. RG1 and RG4 do not have locks. You need to determine how to move resources between resource groups during the lifecycle of these resources. Assuming all resources provisioned support moving between resource groups regardless of region, which of the following statements are plausible?

- You can move resources from RG2 to RG4.

Selected

You cannot move resources from RG2 to RG3, because RG2 has a Read-Only lock. While you can move resources into RG2, you cannot move them out due to the Read-Only lock. The lock would need to be removed in order to be able to move resources out of RG2.

- You can move resources from RG2 to RG3.

- You can move resources between any of these resource groups.

- You can move resources from RG1 to RG4.

Selected

You can effectively move resources from RG1 and RG4, because RG1 does not have a lock.

- You can move resources from RG4 to RG3.

You can move resources from RG4 and RG3, because RG4 does not have a lock. Also, while RG3 does have a Delete lock ,this does not stop resources from being moved into this resource group.

You have just purchased the domain name arseemagroup.com from a third-party registrar. Using your Azure Active Directory domain, you'd like to create new users with the suffix @arseemagroup.com. Which 3 things must you do?

- Verify that you own the domain name

Selected

When you add your custom domain to Azure AD, you must verify that this domain belongs to you by going through a verification process. Azure AD will provide the verification information.

- Access the App registrations blade from Azure AD

- Access the Custom Domain Names blade from Azure AD

Selected

In order to add the domain arseemagroup.com to Azure AD, you must add it from the Custom Domain Names blade.

- Create an MX or TXT record for the arseemagroup.com DNS

Selected

When you add your custom domain to Azure AD, you must create an MX or TXT record with a destination address (provided) in order to verify that the domain does indeed belong to you.

You recently signed up for Azure Active Directory Premium and need users to be able to reset their passwords if they are unable to log in. What should you configure in Azure Active Directory?

- User password reset

Selected

With the password reset capability, the user will be able to click "Forgot Password" when trying to log in to the portal and reset their password on their own.

- User password change.

- Add users to sign-in group in Azure AD

- Set "Block Sign In" to off when creating the user

QUESTION 14

Your company has recently added a few new users to your Azure Active Directory. You have already added them to a security group, and now you have asked them to join their devices to the tenant. When they join their devices, you have to ensure they are prompted to use a mobile phone to verify their identity. What is the simplest way to configure this functionality?

- Sign up for Azure AD Premium

- Configure a point-to-site VPN

- Require multi-factor authentication to join devices

Selected

This setting in Azure Active Directory will require multi-factor authentication for all devices under any conditions.

- Enable conditional access

  Rate this question

You want to provide an Azure AD B2B guest user the ability to manage resources inside of the DevRG resource group. You want to give them the ability to manage all resources inside of this resource group and nothing more. Assuming you are assigning the role to the DevRG scope, which role would you assign to the user to accomplish this goal?

Global Admin

Owner

Contributor

Selected

This role will give this guest user the ability to manage all resources inside of the DevRG resource group and nothing more, like managing role assignments. This is exactly what you need for this scenario. Remember, when assigning permissions, you need to think the principle of least privilege.

User Access Administrator

QUESTION 29

You work at the IT help desk for Consilium Corporation. You have been getting an influx of calls into the help desk about resetting users' passwords. They keep reporting that they can't seem to figure out how to reset their password in order to gain access to their Customer Relationship Management (CRM) software. What do you do?

Make sure you have Azure Active Directory Free.

Ensure that the users who are having problems are within the correct AD group.

Selected

Self-service password may not apply to those outside of a specific Active Directory group. Only users in the group may reset their own passwords.

Make sure they have their verification device (mobile app or access to email).

Selected

In order to reset their password, the user will have to verify their identity using a mobile phone, mobile app, office phone or email.

Issue a document to inform users of password reset procedure.

Selected

If the Active Directory users are not authorized to reset their password, or the Active Directory environment is not suited for this functionality (e.g. licensing), the document in of itself may not help in this situation, but it is a good start.

Good communication is a good idea, but also make sure the users can use self-service in Azure Active Directory.

Verify that self-service password reset is enabled in Azure Active Directory.

Selected

Self-service password reset is an optional feature in Azure Active Directory, which may not apply to all users in the organization.

QUESTION 56

You are working for Cloud Chase Support. You are the active administrator, and have been tasked with determining how to ensure you do not incur costs in either the Prod-Subscription or Dev-Subscription for virtual machine resources. You have a CloudChase management group where both subscriptions are nested. You decide to use Azure Policy to enforce compliance on virtual machines. The Policy definition states that virtual machines are not an allowed resource type at the scope of the CloudChase management group. There are some existing virtual machines in the Prod-Subscription at the time this policy is created. After the enforcement of the new policy, which of the below statements is true?

- You can create virtual machines in Dev-Subscription.
- You cannot create virtual machines in any subscription under the scope of the management group and any existing virtual machines will be deallocated.
- You can create virtual machines in Prod-Subscription if they are compliant.
- You cannot create virtual machines in any subscription under the scope of the management group. Selected

You created a policy that has a definition that states that virtual machines are not a supported resource type at the scope of the CloudChase management group. Therefore, any subscription under the scope of this management group will not support the provisioning of virtual machine resources.

 **DOMAIN**
71% **Implement and Manage Azure Storage**

The Azure Storage platform is Microsoft's cloud storage solution for data storage scenarios. Core storage services offer a massively scalable object store for data objects, disk storage for Azure virtual machines (VMs), a file system service for the Cloud, a messaging store for reliable messaging, and a NoSQL store. We can replicate data across datacenters or geographic regions, secure our data with encryption, and access our data anywhere in the world over HTTP or HTTPS.

Questions for this domain comprise **12% of the total questions** for this exam.

QUESTIONS

10 11 12 13 14 15

QUESTION 19

You work as an Azure Administrator for a film production company. The company stores all of its video clips in file servers on-premises. You are curious about extending the capacity of these on-premises file servers. What Azure Storage service could you utilize to ensure that these on-premises file servers are supported in this way?

- Azure Queue
- Azure Blob
- Azure File Sync Selected

Azure File Sync is used to extend the capacity for on-premises file servers using Azure file shares. You could use Azure File Sync to accomplish this goal.
- Azure Files Selected

Azure Files itself is not used to extend on-premises file servers. Azure Files provide a cloud-managed file share.

 Rate this question

QUESTION 42

The Blob service in Azure Storage can be used to store virtual hard drive (VHD) files. What type of blob would these files be stored as in the Blob service?

Block blobs

Selected

Block blobs are used to store objects such as text files, images, and videos. It is not used to store VHD files.

Page blobs

Page blobs are intended for storing such file types as VHD files and serve as disks for virtual machines.

VHD blobs

Append blobs

Your organization has several offices across the United States. It utilizes file servers to provide a shared endpoint for departments within the organization. The organization wants to migrate to the cloud. Which of the following Azure services would replace the on-premises file servers?

Azure Files

Selected

Azure Files is used to replace on-premises file servers as it is a cloud-managed file share service. This is the service that you could utilize to replace the organization's on-premises file servers.

Azure Tables

Azure Blob

Azure File Sync

Which of the following provide unlimited access to storage accounts in Azure and should never be shared or stored in application code?

- Account SAS tokens
- Service SAS tokens
- Service endpoints
- Access keys Selected

Access keys can be used to provide unlimited access to storage accounts.

You have a general-purpose v1 storage account named `consiliumstore` that has a private container named `container2`. You need to allow read access to the data inside `container2`, but only within a 14 day window. How do you accomplish this using the Azure portal?

- Create a shared access signature (SAS)

Selected

A shared access signature (SAS) allows you to have granular control over your storage account, including access to only certain services (i.e. Azure Blobs) and permitting only read, write, delete, list, add, or create access.

- Upgrade the storage account to general-purpose v2

- Create a service shared access signature (SAS)

- Create a stored access policy

Selected

A stored access policy allows granular control over a single storage container using a shared access signature (SAS).

QUESTION 49

You create an Azure storage account named `consiliumstore` with a publicly accessible container named `container1`. You upload a file to `container1` named `pic1.png`. What will be the URL used in order to access this blob?

- <https://pic1.consiliumstore.blob.core.windows.net>

- <https://portal.azure.com/consiliumstore.blob.core.windows.net/pic1.png>

- <https://consiliumstore.blob.core.windows.net/container1/pic1.png>

Selected

By default, the URL of the blob will be the storage account name, followed by `blob.core.windows.net`, the container name, and then the name of the blob.

- <https://blob.core.windows.net/consiliumstore/container1/pic.png>

QUESTION 59

You work for a company that provides a streaming service for entertainment purposes. You have been storing your video files on-premises in storage servers. Your CTO has advised you that the company is migrating to the cloud, and you have been tasked with investigating which service best fits the organization's use case. You are looking for a service that allows the company to save cost by utilizing lifecycle management. Which of the following Azure services would you select to store these video files for streaming?

Azure Queue

Azure Blob

Selected

Azure Blob storage is an object-based storage solution designed to store block blobs such as video files, and Blob storage supports lifecycle management features for cost savings.

Azure Tables

Azure Files

63%

DOMAIN

Deploy and Manage Azure Compute Resources

Compute resources in Azure refer to the resources that your application runs on. This includes Azure VMs, Azure App Service, Azure Kubernetes Service (AKS), and Azure Container Instances (ACI). Azure services fall into two categories: infrastructure as a service (IaaS) and platform as a service (PaaS). IaaS lets us provision individual VMs along with the associated networking and storage components. Then, we can deploy any software or applications we wish on that VM. PaaS goes even further in removing the need to worry about maintaining the virtual machine hosting our software or applications. Azure App Service is a PaaS service that allows us to run software or applications on infrastructure Azure maintains. Questions for this domain comprise **27% of the total questions** for this exam.

QUESTIONS

17	18	31	50	52
54	7	13	22	25
32	36	40	47	51

QUESTION 17

You have an Azure subscription that contains the following unused resources:

- Network interface (nic0)
- Static public IP (pip1)
- Standard load balancer (lb1) with 5 rules configured
- Virtual network (VNet2) = 10.1.0.0/16
- Stopped (deallocated) virtual machine (VM3)

Which of these unused resources should you remove to lower cost?

Virtual network (VNet2)

Network interface (nic0)

Stopped (deallocated) virtual machine (VM3) Selected

Stopped virtual machines (which have been shut down from the operating system of the VM) will still incur charges. However, stopped and deallocated virtual machines (which have been shut down from the Azure portal or via Azure command-line tools) do not continue to incur charges until such time as they are restarted.

Standard load balancer (lb1) Selected

The pricing for a Standard load balancer is based on the number of rules configured (load balancer rules and NAT rules) and data processed. However, there is no hourly charge for the Standard load balancer itself when no rules are configured. Since this load balancer contains rules, it should be removed to save money. Reference Documentation: [Pricing Virtual Machine IP Address Options](#)

Static public IP (pip1)

There is a charge for static public IP addresses irrespective of the associated resource (unless it is part of the first five static ones in the region), so this resource should be removed. Reference Documentation: [Pricing Virtual Machine IP Address Options](#)

QUESTION 18

Which of the following is required to implement Azure Disk Encryption on virtual machines data disks and OS disks?

Azure Key Vault

Azure Key Vault is a required resource when implementing Azure Disk Encryption. Azure Key Vault stores the encryption key for Azure Disk Encryption.

Access keys

Shared access signature (SAS) tokens Selected

SAS tokens are used to provide limited and granular access to storage accounts or services within storage accounts. They are not used for implementing Azure Disk Encryption.

SSH private keys

QUESTION 31

Subscription1 contains an Azure VM named VM1. You have added a data disk to VM1, as well as a new network interface card. You need to create two more Azure VMs just like this one named VM2 and VM3. What is the most efficient way to create VM2 and VM3 that will minimize cost?

- Redeploy VM1 with the new disk and NIC and deploy the template to VM2 and VM3
- Back up the VM and recover to a different region
- Select *Export template* from the VM1 blade, then deploy VM2 and VM3 with that template
 - Exporting the template from a VM is a quick and easy way to take the existing VM settings and automate future deployments.
- Create an image from VM1 and use the image to deploy VM2 and VM3 Selected
 - By creating a VM image, you will be able to deploy as many VMs as you wish using that VM image as a template. However, there are storage costs associated with the VM image.

QUESTION 50

You plan to create an Azure Web App in the East US region. You need to ensure that this web app scales out with demand to prevent downtime. You also need to ensure that the data that resides inside of the application will remain secure and never become exposed to anyone outside of the organization. Which App Service plan SKU will meet these requirements?

- I1
 - The I1 SKU allows your app to run on dedicated hardware, and also provides network isolation on top of compute isolation to protect your app. It also provides the maximum scale-out capabilities.
- B1 Selected
 - The B1 SKU allows your app to run on dedicated hardware, but does not include network isolation, so someone could still access your application via network intrusion.
- SHARED
- FREE

QUESTION 52

You are trying to create a new Azure Kubernetes Service (AKS) cluster from your local workstation. The AKS cluster must contain three nodes and ensure access to the worker nodes in order to troubleshoot the kubelet. You have authenticated to Azure from your local workstation with the Azure CLI. What command will you use to create an AKS cluster named AKS1 with the necessary components inside of the resource group named RG1?

az kubernetes create --name AKS1 --group RG1 --nodes 3 --generate-keys

az aks create -g RG1 -n AKS1 --generate-ssh-keys --node-count 3

The correct command to use for creating an AKS cluster is `az aks create`.

The `-g` and `-n` values are abbreviated syntax for resource group and name, respectively. The `--generate-ssh-keys` flag will create the SSH keys in order to access the worker nodes. The `--node-count` flag will ensure that there are three worker nodes in the cluster.

az kubernetes create --name AKS1 --resource-group RG1 --nodes 3 --generate-keys

az aks create --name AKS1 --resource-group RG1 --nodes 3 --ssh-key-value ~/.ssh/id_rsa.pub

Selected

The correct command for creating an AKS cluster is `az aks create`, with the `-g` and `-n` values used as abbreviated syntax for resource group and name, respectively. The `--generate-ssh-keys` flag will create the SSH keys in order to access the worker nodes. The `--node-count` flag will ensure that there are three worker nodes in the cluster.

Subscription1 contains an Azure VM named VM1 with the following configuration:

- VM Size: Standard_D2s_v3
- Public IP Address: 52.173.36.55
- Resource Group: RG1
- Availability Zone: None
- Location: Japan East
- Disk Type: Standard HDD

What are two things you can do to reduce data loss and achieve a 99.9% SLA?

- Create a Recovery Services vault and enable replication for VM1

Selected

Creating a Recovery Services vault will allow you to back up the VM to a different region and location. You will enable replication to ensure that VM data and settings are continually replicated to the backup location for simple recovery.

- Move VM1 to a paired region

- Change the disk type to Premium SSD

Virtual machines with Premium SSD disks qualify for the 99.9% connectivity SLA.

- Place the VM in an availability zone

Selected

Once you have created the VM, the availability zone cannot be changed.

Your organization is planning the deployment of an AKS cluster. You want to ensure that every single pod in the AKS cluster receives a private IP address. Which of the following network configurations would you use to provide this functionality?

- Service endpoint

- Container Network Interface

Selected

Container Network Interface is the network config for AKS clusters that provides an IP address for pods.

- Kubenet

- Microsoft routing

QUESTION 13

You are backing up your virtual machines using Azure Backup. You have 3 resource groups: RG1, RG2, and RG3. Inside of each, you have 2 virtual machines. VM1 and VM2 are located in resource group RG1, and VM3 and VM4 are located in resource group RG2. VM1 and VM3 are located in the West US region, VM2 is located in the South Central US region, and VM4 is located in the East US region. Your Azure Recovery Services vault is located in the West US region and inside of resource group RG3. Which of the following virtual machines can you backup with your existing Recovery Services vault?

VM1, VM2, VM3, and VM4

VM1 and VM3

Selected

The virtual machines must exist within the same region as the Recovery Services vault in order to back them up.

VM1 and VM4

QUESTION 22

You have created an application named ContainerApp1 that is to be run on Linux containers. You've created an Azure container instance with an FQDN, but you notice that when the container restarts, all application data is lost. What is the best solution to preserve the data associated with your application?

Run the container on a VM, and use the managed disk attached to the VM

Create a public blob storage container and share the URI with the application

Mount an Azure file share as a volume in Azure Container Instances

Selected

Azure Container Instances can mount an Azure file share created with Azure Files. Azure Files offers fully managed file shares hosted in Azure Storage that are accessible via Server Message Block (SMB) protocol. Using an Azure file share with Azure Container Instances provides file-sharing features similar to using an Azure file share with Azure virtual machines.

Create a storage account and share the SAS with the application

QUESTION 25

You have an Azure subscription that contains the following virtual machine scale set named `myScaleSet`:

InstanceId	LatestModelApplied	Location	ModelDefinitionApplied	Name
0	True	southcentralus	VirtualMachineScaleSet	
1	True	southcentralus	VirtualMachineScaleSet	
3	True	southcentralus	VirtualMachineScaleSet	
5	True	southcentralus	VirtualMachineScaleSet	

You need to remove instance ID 5 from the virtual machine scale set. Which of the following commands should you use?

- `Remove-AzVmssVMDataDisk -VM $VirtualMachine -Lun 0`
- `az vmss deallocate --instance-ids 5 --name myScaleSet --resource-group testgroup` Selected

The `az vmss deallocate` command will deallocate and remove the VMs within a VMSS. `az vmss Commands`
- `az scale set remove --instance-ids 3 --name myScaleSet_5 --resource-group testgroup`
- `Remove-AzVmss -ResourceGroupName "testgroup" -VMScaleSetName "myScaleSet"`

Reviewing the template, what would we modify to ensure that we launch the VM using an Ubuntu 18.04 LTS image version rather than 16.04.0-LTS?

- By changing the default value of our `ubuntuOSVersion` parameter to `18.04-LTS`
- Select the OS version during deployment of this template
- Replace the variable value for `OSVersion` with `18.04-LTS` Selected

By modifying the `OSVersion` variable, we can specify the ubuntu OS version that is being passed into the `resources` section of this template.
- Removing the `variables` section

QUESTION 36

You have decided that you want to create 2 AKS clusters. Each of the clusters has different networking requirements. ClusterAlpha needs each pod to have a private IP address. ClusterBravo requires that each node has a private IP address. Which of the following options would you select for a networking configuration that satisfies the requirements of ClusterBravo?

Kubenet

Selected

Kubenet can provide a private IP for each node in a cluster, which will meet the requirements for the ClusterBravo cluster.

Container Network Interface

Azure Private Link

Private endpoint

QUESTION 40

Your company has decided to use virtual machines as the compute resource for hosting the organization's latest application. To do so, you need to have storage on the virtual machine that provides persistent storage. Which of the following options would you use?

Data disk

Selected

Data disks are managed disks that can be added to existing VMs and used for persistent storage. The data stored on a data disk survives a VM that has been deallocated and can be moved to other VMs.

Containers

Temporary disk

Other

You are currently using a load balanced availability set containing 2 virtual machines. These virtual machines are balanced behind a Basic SKU load balancer. You notice that these 2 virtual machines do not properly serve your workload during peak hours when traffic is way up. You need a solution that will allow you to add virtual machines on the fly when they are needed. Which of the following would provide the most effective solution?

- Create a scale set and use it to replace the backend pool. Selected

Using a scale set with a Basic SKU load balancer would properly support your traffic. You have to replace the backend pool because Basic SKU load balancers support backend pools with either VMs in a single availability set or a scale set.
- Add a virtual machine scale set to the backend pool.
- Upgrade the Basic SKU load balancer to a Standard SKU.
- Add another virtual machine into the availability set.

SOLUTION

You are deploying a virtual machine, and you want to configure the VM on launch without having to make a connection to the VM. Which of the following can you use to configure the VM in this way?

- Custom data Selected

You can use custom data to provide launch configuration details to your VMs.
- Console
- VM Extensions
- VHD Template

 Rate this question

VM1 is a D-series Linux virtual machine in an availability set, which has availability across two fault domains and five update domains. VM1 experiences a hardware failure, but the memory is preserved and doesn't require a reboot. What will happen to the VM when this event occurs?

- Since the memory is preserved, the VM will migrate to all new hardware, except for the memory component.
- The VM will be decommissioned and a support ticket will be automatically generated. You will have to call support in order to retrieve the data from your VM.
- Azure will keep the VM running on the same hardware because fault domains are in place for the VM.
- Azure will migrate VM1 from failing hardware to a healthy physical host and the VM will be paused for up to five seconds. Selected

Azure uses Live Migration technology to migrate virtual machines from the failing hardware to a healthy physical machine. Live Migration is a VM preserving operation that only pauses the virtual machine for a short time. Memory, open files, and network connections are maintained, but performance might be reduced before and/or after the event.

DOMAIN

Configure and Manage Azure Networking Services

65%

The networking services in Azure provide a variety of capabilities, including connectivity services, application protection services, and application delivery services. Virtual Network (VNet), Virtual WAN, ExpressRoute, VPN Gateway, Virtual Network NAT Gateway, Azure DNS, Peering Service, and Azure Bastion are all services available for connectivity in Azure. Private Link, Firewall, Network Security Groups, Web Application Firewall, and Virtual Network Endpoints are all services available for application protection in Azure. Content Delivery Network (CDN), Internet Analyzer, and Load Balancer are all services available for application delivery in Azure. Questions for this domain comprise **32% of the total questions** for this exam.

QUESTION 6

You have an on-premises environment, as well as your Azure environment with a subscription named Subscription1. Subscription1 has a virtual network named VNET1 that you need to connect to the on-premises network securely using an ExpressRoute link and Site-to-Site VPN. What resources do you need in order to establish the connection while minimizing cost?

- A VPN gateway Selected

IPsec VPN tunnels are created between the Azure VPN gateway and the on-premises VPN device. In this case, you do not want to use a VPN gateway for the sake of minimizing cost.
- A route table

A route table is required to specify the next hop for traffic coming and going from the on-premises network.
- No resources are needed, as ExpressRoute is encrypted by default
- A network virtual appliance Selected

VPN tunnels over Microsoft peering can be terminated either using VPN gateway or using an appropriate network virtual appliance (NVA) available through Azure Marketplace. While both will accomplish the goal of establishing a connection between environments, an NVA will incur less cost than a VPN gateway.

Rate this question

-

You have an Azure subscription named Subscription1. In Subscription1 you have 2 VNets: one named VNet-Hub and one named VNet-Spoke. Within VNet-Hub, there is an Azure Firewall with a public IP address, configured as a Standard SKU. In VNet-Spoke, there is a Windows Server 2016 with no public IP address and no network security group (NSG). With which of the following can you utilize the public IP address of the Azure Firewall to connect to the Windows Server without exposing the server to the public internet directly?

- Virtual network peering

In order for traffic to flow from the VNet-Spoke to VNet-Hub, you will need a peered connection between the virtual networks.

- A virtual network gateway

Selected

A virtual network gateway is used to send encrypted traffic between an Azure virtual network and an on-premises location over the public internet. This would not achieve the goal of connecting to the Windows Server using the Azure Firewall public IP address.

- An ExpressRoute gateway

Selected

An ExpressRoute gateway is used to connect an Azure virtual network and your on-premises network. This will not achieve the goal of connecting to the Windows Server using the Azure Firewall public IP address.

- A NAT rule for the Firewall

You can configure a NAT rule on the Azure Firewall to translate and filter inbound internet traffic to your subnets.

- A route table

Selected

You will need a route table to route ingress traffic to the Azure Firewall's virtual appliance.

You are implementing a load balancing solution for your application, and you want it to provide multisite capabilities. Which of the following will provide you with the appropriate solution?

App Service

Azure WAN

Application Gateway

Application Gateway is used to balance traffic between backend pools, and it provides multisite load balancing capabilities.

Azure Load Balancer

Selected

While Azure Load Balancer is used to balance traffic for a backend pool of compute resources, it is not used to balance traffic for a multisite backend solution.

You need to create an Azure virtual machine named VM1 that requires a static private IP address configured inside the IP address space for the VNet in which the VM resides. How do you configure a static IP address for this Azure VM?

When creating a VM in the portal, select **New** next to *Private IP Address* and choose **static** after assigning the correct IP address.

When creating the VM in the portal, change the setting from **dynamic** to **static** Selected on the *Networking* tab under *Private IP Address*.

There is no such option when creating a VM in the Azure portal.

After the VM has been created, go to the network interface attached to the VM and change the IP configuration to **static assignment**.

Changing the IP configuration on the network interface will achieve this goal.

After the VM has been created, create a new network interface and configure a static IP address for that network interface.

You have a subscription named Subscription1. Subscription1 has two virtual networks named VNet1 and VNet2 in two different resource groups. VNet1 is located in the West US region and VNet2 is located in the East US region. You need to apply a network security group named NSG1 to a subnet in VNet1. NSG1 is located in the East US region. How do you attach NSG1 to the subnet in VNet1?

- You can not attach NSG1 to the subnet in VNet1. Create a new network security group in the West US region

In order for you to associate a network security group to a subnet, both the virtual network and the network security group must be in the same region.

- Move NSG1 into the VNet1 resource group
- Select the subnet and choose NSG1 from the network security group drop-down
- Move VNet1 into a resource group located in the East US region

Selected

Moving the virtual network into a different resource group will not have an effect on the network security group association.

You have an Azure subscription named Subscription1. In Subscription1 you have an Azure VM named VM1 with Windows Server 2019 as the operating system. VM1 does not have a public IP address assigned to it. VM1 is located in a virtual network named VNet1, in subnet1.

Attached to subnet1 is a network security group (NSG) that has port 3389 open inbound. On your local machine, you do not have an RDP client installed, but you need to log in to the VM. Without assigning a public IP address to the VM, what three things in combination could you use to log into VM1?

- A HTML5-supported web browser

The RDP connection to the virtual machine happens via Bastion host in the Azure portal (over HTML5) using port 443 and the Bastion service.

- A subnet named **AzureBastionSubnet**

Selected

The subnet inside your virtual network to which the Bastion resource will be deployed must have the name **AzureBastionSubnet**. The name lets Azure know which subnet to deploy the Bastion resource to.

- An inbound security rule to open port 443

Selected

Allowing inbound port 443 is not required because the RDP session will open directly in the Azure portal (over HTML5) using port 443 and the Bastion service.

- An Azure Bastion host

Selected

The Azure Bastion service is a fully platform-managed PaaS service that you provision inside your virtual network. It provides secure and seamless RDP/SSH connectivity to your virtual machines directly in the Azure portal over TLS. When you connect via Azure Bastion, your virtual machines do not need a public IP address.

- An Azure VPN gateway

- A gateway subnet

You have an Azure subscription that contains 3 virtual machines that run Windows Server 2016 and are configured as follows:

Name	PublicIP	PrivateIP	VNet	Name	DNSuffix
VM1	65.74.185.47	192.1.0.4	VNET1	consilium.com	
VM2	47.185.85.63	10.1.0.4	VNET2	axiodata.com	
VM3	66.166.78.43	192.1.0.5	VNET1	consilium.com	

You create a public DNS zone named consilium.com and a private DNS zone named axiodata.com

In the settings for the private DNS zone, you create a virtual network link to VNET2 and enable auto registration. What will happen to VM2 when it starts up?

- A record for VM2 will be added to the axiodata.com DNS zone only once you configure the DNS servers for VNET2Selected

Once you link the virtual network and turn auto registration on, Azure DNS updates the zone records automatically when a machine is created, changes its IP address, or is deleted.
- A record for VM2 will be added to the consilium.com DNS zone
- A record for VM2 will be added to the axiodata.com DNS zone

Any existing virtual machines and any new VMs added to VNET2 will be auto registered and a record will be added in the axiodata.com DNS zone.
- A record for VM2 will be added to both consilium.com and axiodata.com

The Consilium Company has just deployed a number of Azure VMs into a specific subnet in an Azure virtual network. They have also implemented a network security plan which includes the use of Azure Firewall. From those newly deployed VMs, the company wants to deny access to the website <https://www.microsoft.com>. How can you achieve this using their current Azure resources?

- A network security group rule Selected
 - A network security group rule could deny access to the IP addresses that correspond to www.microsoft.com. A better way though would be to use an application rule on the Azure Firewall that blocks the FQDN for www.microsoft.com.
- An Application Gateway
- A route via Route Table to the firewall (as a virtual appliance hop) Selected
 - This is required to direct incoming traffic (from the firewall's public IP address) to a specific destination.
- A VPN gateway
- A subnet named [AzureFirewallSubnet](#)
- An application rule on the Azure Firewall that blocks FQDN www.microsoft.com Selected
 - An application rule allows or blocks an address by URL. This is necessary in order to block <https://www.microsoft.com> according to the requirements of the company.

You have 2 virtual networks named VNet1 and VNet2. VNet1 is located in the West US region whereas VNet2 is located in the East US region. You need to configure a virtual machine that's located in VNet1 to also communicate with VMs in VNet2. From the choices available, how can you enable communication between resources in VNet1 and VNet2?

- Configure a VNet-to-VNet VPN gateway connection to allow communication between VNets in different regionsSelected

VNet-to-VNet connections allow communication between virtual networks in different regions and from different subscriptions. Reference Documentation: [Configure a VNet-to-VNet VPN Gateway Connection by Using the Azure Portal](#).
- Migrate just the VM disks to VNet2
- Migrate the VNet1 VM to VNet2 and leave the other VM components on VNet1
- Migrate the network interface card (NIC), the network security group (NSG), and the VM disks to VNet2

Which of the following Network Watcher tools could you use to investigate all traffic between VM1 and VM2 for a duration of 3 hours?

- VPN diagnostics
- Packet captureSelected

The packet capture tool can be used to investigate all traffic between VM1 and VM2 for a duration of time.
- IP flow verify
- Connection troubleshoot

You have a web application that serves video and images to those visiting the site. You start to notice that your web server is overloaded, and often crashes because the requests have consumed all of its resources. To combat this, you've added an additional web server, and you plan to load balance these servers by serving images from the first server only and serving video from the second server only. Which Azure resource can you implement that will properly load balance (at OSI layer 7) with URL-based routing and secure with SSL at the lowest cost?

- Azure Application Gateway

Selected

Azure Application Gateway operates at layer 7 (the application layer), and is a web traffic load balancer that enables you to manage traffic to your web applications. Application Gateway can make routing decisions based on URI path and secure with SSL.

- Web Application Firewall
- Azure Load Balancer
- Azure Front Door

Which of the following tools allows you to determine the traffic that is allowed and/or denied inbound or outbound from a virtual machine?

- Next hop
- Connection monitor

- IP flow verify

Selected

IP flow verify is the Network Watcher diagnostic tool that you can use to determine the traffic that is allowed and/or denied inbound or outbound from a VM.

- Packet capture

QUESTION 12

You have two virtual networks, VNet1 and VNet2. VNet 1 has an IP CIDR of 10.0.0.0/16, and VNet2 has an IP CIDR of 192.168.0.0/16. You want to be able to communicate between these virtual machines privately over the Microsoft backbone. Which of the following could you use to accomplish this without transitivity to other potentially peered networks?

- Azure WAN
- VPN gateway
- ExpressRoute
- VNet peering

Selected

VNet peering can be configured between these VNets with non-overlapping IP CIDRs. Once the peering connections are created on both sides of the peering, these VNets will be able to communicate privately without transitivity to potentially peered networks.

You have two Azure virtual machines named VM1 and VM2. VM1 is using the Red Hat Enterprise Linux 8.1 (LVM) operating system and is located in VNet1, within subnet1. VM2 is using the Windows Server 2019 operating system and is located in VNet1, within subnet2. VNet1 has custom DNS configured, pointing to a DNS server with the IP address 172.168.0.6. VM2 has 10.0.1.15 configured as the DNS server on its network interface. Which DNS server will VM2 use for DNS queries?

- 8.8.8.8
- 10.0.1.15 for primary, 172.168.0.6 as secondary
- 172.168.0.6
- 10.0.1.15

Selected

Since the network interface attached to VM2 is assigned to a specific DNS server, it takes precedence over the DNS configured on the VNet.

You have an Azure subscription and an on-premises environment that are connected via ExpressRoute circuit. You have two additional branch offices that you need to connect to the network, as well as 10 remote employees that change locations frequently but still need access to Azure resources. What is the solution that will provide the quickest setup at the lowest cost?

Virtual WAN

Selected

The Virtual WAN architecture is a hub-and-spoke architecture for branches and users. It enables global transit network architecture, where the cloud-hosted network "hub" enables transitive connectivity between endpoints that may be distributed across different types of "spokes". All hubs are connected in full mesh in a standard Virtual WAN, making it easy for the user to use the Microsoft backbone for any-to-any (any spoke) connectivity. This satisfies the requirement to provide the quickest set up at the lowest cost.

Hub-and-spoke network topology

Point-to-Site VPN

Site-to-Site VPN

Which of the following load balancing configurations can you utilize to ensure that the same virtual machine in the backend pool services the same client?

- Session persistence

Selected

Session persistence is the configuration that you set on your load balancers to ensure that the same virtual machine in the backend pool services the same client.

- Health probe

- NAT rule

- Load balancing rule

QUESTION 45

You have an Azure subscription named Subscription1. You would like to connect your on-premises environment to Subscription1. You have to meet three requirements from the business. The first requirement is that the connection from the on-premises office and Azure must be a private connection. No network traffic is allowed to go over the public internet. The second requirement is that all traffic from the on-premises office and Azure must happen at layer 3 (network layer). The third requirement is that this connection from on-premises to Azure must be redundant to minimize the opportunity for failure. What type of connection fulfills these three requirements?

- ExpressRoute with Premium add-on

- Virtual WAN

- ExpressRoute

Selected

ExpressRoute lets you extend your on-premises networks into the Microsoft cloud over a private connection facilitated by a connectivity provider. ExpressRoute connections do not go over the public internet. An ExpressRoute connection is a layer 3 connection between your on-premises network and Azure through a connectivity provider (e.g. Verizon). The customer and the service provider segments of ExpressRoute connectivity need architected for high availability.

QUESTION 46

You have a standard load balancer that directs traffic from port 80 externally to 3 different virtual machines. You need to direct all incoming TCP traffic on port 5000 to port 22 internally for connecting to Linux VMs. What do you need in order to connect to the VM via SSH?

A route table with at least one rule

A network security group (NSG)

Selected

The NSG rules work alongside the NAT rules to provide a connection to a VM that's behind a load balancer.

A public IP address for all 3 VMs

A Network Address Translation (NAT) rule

Selected

NAT rules work alongside NSG rules to provide a connection to a VM that's behind a load balancer.

You have a small number of servers running a microservice, and you want to make sure that all the servers have connectivity with each other. You also need to calculate network performance metrics like packet loss and link latency. Which 2 Azure resources do you need to meet this requirement?

Network Watcher Agent

Selected

To make Connection Monitor recognize your Azure VMs as monitoring sources, you need to install the Network Watcher Agent virtual machine extension on them. Azure virtual machines require the extension to trigger end-to-end monitoring and other advanced functionality.

Connection Monitor

Selected

Connection Monitor provides unified, end-to-end connection monitoring in Azure Network Watcher and supports hybrid and Azure cloud deployments. Connection Monitor provides support for connectivity checks that are based on HTTP, Transmission Control Protocol (TCP), and Internet Control Message Protocol (ICMP).

Azure Monitor

Azure Traffic Manager

You are responsible for 3 virtual networks named Spoke1, Spoke2, and Hub. You need to ensure that resources within Spoke1 can communicate with resources in Spoke2. You also need to ensure that all communication from Spoke1 to Spoke2 is private. Due to company policy, you cannot connect Spoke1 to Spoke2 directly. What can you do to reach this requirements?

- ✗ Create a firewall rule to allow traffic from Spoke1 to Spoke2 using the Hub VNet.
- ✗ Create three virtual network gateways to enable connections between Spoke1 and Spoke2 through the Hub VNet.
- ✓ Create a peering between each Spoke VNet and the Hub VNet. Deploy a network virtual appliance in the Hub VNet and configure routes to forward traffic between Spoke1 and Spoke2 through the network virtual appliance. Selected
 - Virtual network peering is a non-transitive relationship between two virtual networks, so the connection is private. The network virtual appliance deployed in the Hub VNet can forward traffic from Spoke1 to Spoke2 through the Hub VNet. [Create a peering](#).
- ✗ Create a private endpoint from the Hub VNet to enable traffic between Spoke1 to Spoke2.

DOMAIN
Monitor and Backup Azure Resources
71%

Disaster recovery is an important component of Azure. When problems occur, you must be ready to implement the correct solution, whether that's interpreting metrics to determine potential failure or performing restore operations using Azure Backup service. These questions will test your knowledge of when and where to configure monitoring to ensure the longevity of your data in Azure. Questions for this domain comprise **12% of the total questions** for this exam.

QUESTIONS

38	45	8	10	23
33	53			

QUESTION 38

You have an Azure virtual machine running Windows Server 2016. You need to collect OS level metrics on this virtual machine, including Windows event logs and performance counters. Which of the following items do you need in order to collect this metrics data?

- ✓ Storage account for diagnostics data Selected
 - In order to enable guest-level monitoring, you need to create a storage account for storing the metrics data.
- ✗ InfluxData Telegraf Agent
- ✓ Guest-level monitoring Selected
 - In order to install the Azure Performance Diagnostics VM Extension for Windows on an Azure VM, you must enable guest-level monitoring from the VM settings in the portal.
- ✗ Log Analytics agent Selected
 - The Log Analytics agent is not required in this case. If you were to send collected data for analysis over a period of time, then Log Analytics would be more applicable.
- ✓ Azure Performance Diagnostics VM Extension for Windows
 - Azure Performance Diagnostics VM Extension for Windows is an agent in Azure Monitor that collects monitoring data from the guest operating system and workloads of Azure virtual machines and other compute resources.

Rate this question

You have an Azure subscription with a virtual machine named VM1. You are using a Recovery Services vault (RSV) to back up VM1 with soft delete enabled. The backup policy is set to back up daily at 11 PM UTC, retain an instant recovery snapshot for 2 days, and retain the daily backup point for 14 days. After the initial backup of VM1, you are instructed to delete the vault and all of the backup data. What should you do?

- Wait 15 days before deleting the data
- Wait 14 days before deleting the data
- Delete Backup Jobs Workload
- Stop the backup of VM1 and delete backup data

Selected

If you stop the backup of VM1 and choose **Delete backup data** from the dropdown menu, this will stop future backups and delete the existing backup data.

- Turn off soft delete in the vault security settings

When you stop the backup and delete the backup data, because you have soft delete enabled, the backup data is still kept. Permanently deleting the soft-deleted backup items would remove the backup data indefinitely.

- Delete the backup policy

Selected

Once you have stopped the backup, the backup policy is no longer applied. Therefore, deleting the backup policy will have no effect on the outcome you seek in this scenario.

You have a subscription named Subscription1. You would like to be alerted upon certain administrative events within Subscription1 to detect unauthorized access. Which of the following is the quickest method to set up these types of alerts?

- Monitor > Alerts > New Alert Rule Selected
 - Alerts can be created from within Azure Monitor.
- Policy > Assignments > Assign Policy
- Log Analytics Workspace > *myWorkspace* > Advanced Settings
- Subscriptions > *mySubscription* > Activity Log > New Alert

QUESTION 10

The lead infrastructure engineer on your IT team has reached out to you as a cloud engineer to investigate a backup solution for your Azure VMs. You have already begun implementing a solution by first creating an Azure Recovery Services vault. Which of the following would you do next to implement a backup solution?

- Create a backup policy Selected
 - Since you have already created a Recovery Services vault, the next logical step is to configure the backup policy for the backup solution.
- Configure a recovery plan
- Take your first VM backup
- Enable Site Recovery

You have an Azure subscription named Subscription1. In Subscription1 you have two Azure VMs named VM1 and VM2, both running Windows Server 2016. VM1 is backed up using a Recovery Services vault, with a backup policy configured to produce a daily backup and keep that daily backup for 7 days. Also, a snapshot is kept for 2 days. VM1 is compromised by a virus that infects the entire system, including the files. You need to restore the files from yesterday's backup of VM1. What method can you use to restore the files to in the quickest manner?

- Create a new Azure VM and restore to it
- Restore from VM2
- Restore in-place
- Restore the VM1 snapshot

Selected

Using snapshots for VM backups, you speed up the recovery time considerably. The snapshots are stored with the disks in Azure, so the transfer speeds are optimal.

QUESTION 33

You have two subscriptions, one named Subscription1 and the other named Subscription2. Both subscriptions are located within the same tenant. You have one Azure virtual machine located within Subscription1 and another Azure virtual machine within Subscription2, and you'd like to view CPU utilization metrics on both virtual machines. How can you achieve this while maintaining the minimum number of Azure resources and minimizing cost?

Enable guest-level monitoring on each VM

Create a Log Analytics workspace for both VMs

Selected

You can view metrics data (such as CPU utilization percentage) over time by sending your metrics data to a Log Analytics workspace. This workspace can collect metrics data from multiple VMs, no matter if they are located in the same or different subscriptions.

Turn on VM insights in Azure Monitor

Selected

VM insights integration with Azure Monitor Logs delivers powerful aggregation and filtering, allowing Azure Monitor to analyze VM data trends over time. You can view this data in a single VM from the virtual machine directly, or you can use Azure Monitor to deliver an aggregated view of your VMs where the view supports Azure resource-context or workspace-context modes.

Install the Log Analytics agent on the VMs

You are using Azure VMs to host a critical user-facing application. You want to ensure that you have a backup solution prepared for the VM. Which of the following steps would you take first in setting up a backup solution?

Configure Azure Backup

Create a backup policy

Create a Recovery Services vault

Selected

The very first step in setting up a backup recovery solution is creating Recovery Services vault.

Configure a recovery plan

QUESTION 4

You want to provide users within your tenant the ability to register their devices with Azure AD, but you don't want to allow all users to register devices. What can you do to control this?

- Require multi-factor authentication for registering devices.
- Use select administrative units to register devices.

Administrative units are used to control what identity resources Azure AD administrators can manage, not to control registration of Azure AD join.
- It is not possible to restrict which users can register devices.
- Use security groups and allow a select group to register devices.

You can use groups to provide specific users the ability to register their devices with Azure AD.

Selected

Now all you have to do is decide how to assign this policy. You want to stop G series instance from being provisioned across the organization. Which of the following design strategies helps ensure the most effective implementation of this policy, while having the least administrative overhead?

- Create management groups and organize subscriptions into them, then assign the policy to all management groups under the root management group.
- Assign this policy to all of the resource groups throughout the organization.
- Use management groups to organize subscriptions into logical management group containers, where you can then assign the policy to all subscriptions owned by the organization.
- Use management groups to organize subscriptions into logical management group containers, where you can then simply assign the policy to the root management group.

You can accomplish your goal by assigning this policy at the root management group level. From the root management group, all other subscriptions/management groups under the root will inherit this policy.

Selected

As an organization, you want to provide users' access to the storage accounts in Azure so that they will be able to work with data stored in the Blob service. These users are non-technical and prefer a GUI interface. You generate SAS tokens for these users that provide limited access to the storage blobs. What storage utility can these users utilize to access the blobs?

- Export jobs
- Import jobs
- Storage Explorer
 - Storage Explorer is a storage utility that provides a GUI experience.
- AzCopy

QUESTION 18

You have data in an AWS S3 bucket named `myS3Bucket` and you need to copy all of its contents to a container named `container1` in an Azure storage account named `consiliumdata`. Which command would be most efficient for getting the data from the S3 bucket to the Azure storage container?

- `azcopy copy sync 'https://s3.amazonaws.com/myS3Bucket'`
`'https://consiliumdata.blob.core.windows.net/container1'`
- `azcopy blob copy 'https://s3.amazonaws.com/myS3Bucket'`
`'https://consiliumdata.blob.core.windows.net/container1'`
- `aws s3 cp s3://mybucket/test.txt`
`https://consiliumdata.blob.core.windows.net/container1`
- `azcopy copy 'https://s3.amazonaws.com/myS3Bucket'`
`'https://consiliumdata.blob.core.windows.net/container1' --`
`recursive=true`Selected

The AzCopy tool can copy directly from an AWS S3 bucket to an Azure Storage Account. Resource Documentation: [Copy Data from Amazon S3 to Azure Storage by Using AzCopy](#)

QUESTION 7

You have an Azure subscription named Subscription1. You have created a web app named App1 in Subscription1 that is sourced from a Git repository named Git1. You need to ensure that every commit to the master branch in Git1 triggers a deployment to a test version of the application before releasing it to production. What are two changes that you must make to App1 to fulfill this requirement?

- Create a build server with the master branch of Git1 as the trigger

You have the option of creating a build server natively in App Services by selecting *Deployment Center* in the App1 blade. This will trigger a build every time a commit is made to the master branch of Git1.

- Configure custom domains for test and production versions of App1

Selected

Simply creating custom domains will not meet the requirements of deploying to test based on the commit trigger.

- Add a new deployment slot to App1 to release the test version of App1

Selected

Deployment slots allow greater flexibility within app services, providing a built-in staging environment for your app and access to your application without deploying it to production.

- Create a new web app and configure failover settings from test to production

QUESTION 11

VM1 is located in the West US region and the OS disk is Premium SSD. The size of VM1 is currently Standard_D2s_v3, but you need to change the size to Standard_D2. You are able to select the size from the Size blade, but you receive an error message. Why can't you change the VM size?

- You did not shut down (deallocate) VM1 before you changed the size

Selected

You typically don't have to shut down the VM in order to change the VM to certain sizes (though in some cases you do). In this case, you can change the VM size to B1ls, B1ms, B1s, B2ms, B2s, B4ms, D4s_v3, DS1_v2, DS2_v2, or DS3_v2 without shutting down VM1.

- You need to provide the username and password for the OS to upgrade

- Standard_D2 does not support Premium SSD Managed Disks

Standard_D2 does not support Premium SSD Managed Disks; therefore, you are unable to change VM1 to this size. A good way to remember which size is available is the **s** in the size, as the **s** indicates Premium SSD. See more about [Dv3 and Dsv3-Series]](<https://docs.microsoft.com/en-us/azure/virtual-machines/dv3-dsv3-series#dsv3-series>).

- The size Standard_D2 is not available in the West US region

QUESTION 20

Which of the following can you encrypt with Azure Disk Encryption?

- Temporary disks and OS disks

- Only data disks

Selected

While Azure Disk Encryption does support the encryption of data disks, this is not the only type of disk that can be encrypted on VMs.

- Data disks and temporary disks

- OS disks and data disks

Azure Disk Encryption supports the encryption of both the data disks and the OS disks of VMs.

You have an Azure subscription named Subscription1. In Subscription1, you have an Azure virtual machine named VM1, which uses the "Standard_A2_v2" size. Attached to VM1 are two network interface cards. You require a third network interface card with a network bandwidth above 1000 Mbps for your storage area network. What should you do?

- Create a new storage account to store data for VM1
- Create an additional VM in the same subnet and connect to VM1 over the LAN
- Create a new subnet with a sufficient number of available IP addresses
- Change the VM SKU to Standard_A4 or larger

Selected

The larger SKUs for Azure virtual machines allow for an increased number of NICs. [Av2-series](#).

You have created a new Azure virtual machine named VM1. You plan to use VM1 as a web server, which will require the VM to be accessible using HTTP/S (HTTP and HTTPS) protocol. A network security group (NSG) is attached to the NIC of VM1 with the following rules:

Priority	Name	Port	Protocol	SRC	DEST	Action
300	Rule2	80	TCP	Any	Any	Deny
400	Rule1	443	TCP	Any	Any	Deny
500	Rule4	60-500	TCP	Any	Any	Allow
600	Rule5	22	TCP	72.166.177.14/32	Any	Deny
1000	Rule3	22	TCP	Any	Any	Allow

What changes do you have to make to the NSG in order to meet the requirements for VM1?

- Change the priority of Rule4 to 200

Lower priority rules take precedence over higher ones. Changing Rule4 to a lower number will negate all the other rules of a lesser priority, therefore allowing traffic on ports 60-500, which includes 80 and 443, the ports necessary for allowing traffic over HTTP/S. Remember the lower the priority number, the higher the priority in regards to reading the rules.

- Change the priority of Rule3 to 200
- Change the action of Rule1 to Allow
- Change the port of Rule5 to 443

You are currently using three virtual machines as the compute solution to host a public facing e-commerce website in Azure. Recently, you had an issue with two virtual machines going down related to an underlying host failure. Your company lost a lot of business during this outage. Which of the following could you use to rework your virtual machine solution to protect against underlying host failures?

- Scale sets
- Load balancer
- Availability sets Selected
 - Placing your virtual machines into availability sets will provide your VM workloads with protection from underlying hardware failure and maintenance.
- Data disks

Your company wants to implement a load balancing solution in Azure that provides a 99.99% SLA, but it also wants to minimize costs. Which of the following in combination would provide the most appropriate, cost effective solution?

- Standard Load Balancer Selected
 - Standard Load Balancers provide a 99.99% SLA, whereas Basic Load Balancers do not.
- Backend pool of 1 virtual machine
- Basic Load Balancer Selected
 - Basic Load Balancers do not provide a 99.99% SLA, so they will not meet the requirements of the necessary solution.
- Backend pool of 2 virtual machines
 - A backend pool with 2 virtual machines, when implemented with a Standard Load Balancer, would provide the 99.99% SLA.

QUESTION 15

You are planning out the network design for a VNet where you will be hosting an application with a database layer, logic layer, and a web frontend. How many subnets should you create within this VNet?

3

When planning out a network, you should typically follow an N-tier architecture, which means that you create a subnet for each layer of your application. In this case, since you have 3 layers — the database layer, the logic layer, and the web-front end — you would have 3 subnets.

1

Selected

When planning out a network, you should typically follow an N-tier architecture, which means that you create a subnet for each layer of your application. In this scenario, you have 3 layers which equals 3 subnets, not 1.

4

2

You manage a virtual network named VNet1 that is hosted in the West US region. Two virtual machines named VM1 and VM2, both running Windows Server, are on VNet1. You need to monitor traffic between VM1 and VM2 for a period of five hours.

What solution could you use to meet these requirements?

- Azure SQL Analytics
- Azure Monitor for VMs
- Application Insights Selected

While Application Insights can be used for similar use cases, such as monitoring traffic between endpoints of a solution, it is specifically used for Web App Service, not monitoring traffic between VMs.

- Connection Monitor in Azure Network Watcher

The connection monitor capability in Azure Network Watcher monitors communication at a regular interval and informs you of reachability, latency, and network topology changes between the VM and the endpoint. This is the best solution for your use case of monitoring traffic between the two VMs.

Your web application is hosted in a VNet on a virtual machine running Ubuntu LTS and has a public IP address. The virtual machine has a default network security group (NSG) implemented on the network interface (NIC) level. No other NSGs exist in this VNet. However, you are unable to visit the web app hosted on your VM over HTTP. Why?

- You need to allow inbound for port 80 and allow outbound for the ephemeral ports.
- You need to host the app using App Service.
- You need to allow traffic outbound for port 443.
- You need to allow traffic inbound for port 80. Selected

You need to implement a security rule on the NSG that will allow traffic over port 80, which is for servicing HTTP traffic. You only need to create the inbound security rule because NSGs are stateful.

You have two subscriptions named Subscription1 and Subscription2. You are currently managing resources in Subscription1 from Computer1, which has the Azure CLI installed. You need to switch to Subscription2. Which command should you run?

- ✗ `az set account --subscription "Subscription2"`
- ✗ `Select-AzureSubscription -SubscriptionName "Subscription2"`
- ✗ `az subscription set "Subscription2"`
- ✓ `az account set --subscription "Subscription2"`

You are accessing Azure from Computer1 with the Azure CLI installed; therefore, this command is the correct command.

QUESTION 44

You are working for Cloud Chase Support. You are the active administrator, and have been tasked with determining how to ensure you do not incur costs in either the Prod-Subscription or Dev-Subscription for virtual machine resources. You have a CloudChase management group where both subscriptions are nested. You decide to use Azure Policy to enforce compliance on virtual machines. The Policy definition states that virtual machines are not an allowed resource type at the scope of the CloudChase management group. There are some existing virtual machines in the Prod-Subscription at the time this policy is created. After the enforcement of the new policy, which of the below statements is true?

- ✓ You cannot create virtual machines in any subscription under the scope of the management group.
 - You created a policy that has a definition that states that virtual machines are not a supported resource type at the scope of the CloudChase management group. Therefore, any subscription under the scope of this management group will not support the provisioning of virtual machine resources.
- ✗ You cannot create virtual machines in any subscription under the scope of the management group and any existing virtual machines will be deallocated.
- ✗ You can create virtual machines in Prod-Subscription if they are compliant.
- ✗ You can create virtual machines in Dev-Subscription.

Under your Azure subscription, you are trying to identify VMs that are underutilized in order to shut down all VMs with CPU utilization under 5%. Which tool could you use to analyzes your configurations and usage telemetry? You also would like personalized, actionable recommendations to optimize your Azure resources for reliability, security, operational excellence, performance, and cost.

Advisor

Advisor helps you follow best practices to optimize your Azure deployments. It analyzes your resource configuration and usage telemetry and then recommends solutions that can help you improve the cost effectiveness, performance, high availability, and security of your Azure resources.

Monitor

Customer Insights

Metrics

  Rate this question

You have been directed to copy all data from one storage account to another using the AzCopy tool. You need to report which storage services you can copy. Which of those services would it be?

Azure Table and File Shares

Only Azure File Shares

Azure Blob and File Shares

AzCopy is a command-line utility that you can use to copy blobs or files to or from a storage account.

Azure Queues and Blobs

QUESTION 1

Your organization utilizes Azure Files for managed cloud file shares that support multiple offices. Which of the following statements is true?

- Azure Files uses a virtual file structure.
- Azure Files can only be mapped to Windows machines
- You can connect Azure file shares across distros like Linux, Windows, and macOS.
 - Azure Files does support connecting to Linux, Windows, and macOS.
- Azure Files allow you to export data using Azure export jobs.

You've created a Dockerfile that contains the necessary steps to build an image that you plan to use for your application running as a Web App in App Services named APP1. You have created an Azure Container Registry, which is where you plan to store your images to be used for APP1. What should your next step be?

- Run the `docker login` command
- Run the `az acr build` command
 - The `az acr build` command will build and push your image to an Azure Container Registry all in one command. You should use this if you don't have Docker installed, and/or if you don't have the compute resources to build images on your local machine.
- Run the `docker push` command
- Create the App Service Plan

QUESTION 57

You are backing up your virtual machines using Azure Backup. You have 3 resource groups: RG1, RG2, and RG3. Inside of each, you have 2 virtual machines. VM1 and VM2 are located in resource group RG1, and VM3 and VM4 are located in resource group RG2. VM1 and VM3 are located in the West US region, VM2 is located in the South Central US region, and VM4 is located in the East US region. Your Azure Recovery Services vault is located in the West US region and inside of resource group RG3. Which of the following virtual machines can you backup with your existing Recovery Services vault?

- None of the VMs
- VM1 and VM4
- VM1, VM2, VM3, and VM4
- VM1 and VM3

The virtual machines must exist within the same region as the Recovery Services vault in order to back them up.

 Rate this question

You have created a new Azure virtual machine in a subnet named Subnet1 with an attached network interface card named NIC1. The NIC1, attached to Subnet1, has the following effective routes:

Source	State	Address Prefix	Next Hop
Default	Active	10.1.0.0/16	Virtual Network
Default	Invalid	0.0.0.0/0	Internet
Default	Active	10.0.0.0/8	None
Default	Active	100.64.0.0/10	None
Default	Active	192.168.0.0/16	None
Default	Active	25.33.80.0/20	None
Default	Active	25.41.3.0/25	None
User	Active	0.0.0.0/0	None

What will happen when the virtual machine tries to communicate with a VM on a different network?

- Traffic will be sent successfully
- Traffic will be dropped and no connection will be established
 - The user-defined route with a Next Hop type of None in the table will override the default route, causing traffic to be directed to nowhere and the connection to be dropped.
- Traffic will be forced internally
- Traffic will be forced out to the internet

QUESTION 32

Which of the following load balancing configurations checks on the availability of virtual machines in the backend pool of a Basic Load Balancer?

TCP reset

Health probe

A health probe is utilized to check the availability of VMs in the backend pool to ensure they are healthy and can serve traffic distributed from the load balancer.

Session persistence

NAT rule

You have an Azure subscription named Subscription1. In Subscription1, you have a web server that has the IP address 10.1.0.83 and a database server that has the IP address 10.1.0.142. Instead of remembering the IP addresses of the servers, you'd like to connect to these servers using a DNS name. With no DNS server currently, and without having to create a new DNS server, how can you access your database server from your web server by the DNS name db.yourcompany.com?

Use a public DNS zone

Use a private DNS zone

A private DNS zone is an easy way to register servers with a DNS name versus having to access them by their IP address.

Access the domain controller

Promote the web server to a domain controller

Which of the following provides a set of monitoring and diagnostics tools for troubleshooting networks and is enabled on a per-region basis?

- Azure Firewall
- Application Insights
- Network Watcher
 - Network Watcher is the monitoring and diagnostic tool for troubleshooting networks. It is enabled on a per-region basis in your Azure subscriptions.
- Network Insights

QUESTION 27

You have a .NET Core application running in Azure App Services. You are expecting a huge influx of traffic to your application in the coming days. When your application experiences this spike in traffic, you want to detect any anomalies such as request errors or failed queries immediately. What service can you use to assure that you know about these types of errors related to your .NET application immediately?

- Search feature in Application Insights
- Live Metrics Stream in Application Insights
 - Live Metrics Stream includes such information as the number of incoming requests, the duration of those requests, and any failures that occur. You can also inspect critical performance metrics such as processor and memory.
- Log Analytics workspace
- Client-side monitoring

QUESTION 48

You have an Azure subscription named Subscription1. In Subscription1, you have an Azure virtual machine named VM1. In order to create a daily backup of VM1, starting at 11:00 PM and retaining a copy of the backup for recovery purposes for 7 days, what are the 2 items you will need in order to store the backup and configure the schedule?

- A Recovery Services vault

A Recovery Services vault (RSV) is used to store backups of your VMs in a different region.

- A backup policy

A backup policy is used to configure how backups are taken and how often they are kept.

- A batch file

- A cron job

QUESTION 55

Which of the following Azure services enables you to perform disaster recovery solutions by replicating workloads from a source region to a destination region?

- Import/Export jobs

- Azure Site Recovery

Azure Site Recovery is a disaster recovery service used to replicate workloads from a source region to a destination region.

- Azure Backup

- Log Analytics

QUESTION 13

You have an Azure pay-as-you-go subscription named Subscription1. You have some concerns about cost for Subscription1, and you would like to spend less than \$100.00 US per month on all resources in this subscription. If you spend more than \$90.00 US, you would like to get an alert in the form of a text message. What should you do?

- Create a budget in the Subscriptions blade

Selected

Creating a budget ensures that you will be notified when your cost for resources reaches a certain amount, but it will send you the alert via email.

- Shut down VMs when you are not using them

- Create a budget alert condition tied to an action group

Creating an alert condition is available when setting your budget, but is not required that you create an action group. However, in this case, where you want to be notified via SMS (text message), it is required that you tie an action group to our budget alert.

- Create an alert in Azure Monitor

QUESTION 24

You want to provide users within your tenant the ability to register their devices with Azure AD, but you don't want to allow all users to register devices. What can you do to control this?

- Require multi-factor authentication for registering devices.

Selected

Requiring multi-factor authentication for registering devices is an option for improving device registration security, but it doesn't allow you to control which users can register devices using Azure AD join with the AAD tenant.

- Use select administrative units to register devices.

- It is not possible to restrict which users can register devices.

- Use security groups and allow a select group to register devices.

You can use groups to provide specific users the ability to register their devices with Azure AD.

 Rate this question

QUESTION 12

You are the Azure Administrator working for CloudMotive Inc. and you have been tasked with ensuring proper access permissions for all Azure AD users. Adam is the Solutions Architect for the Marketing team. All of the resources for the Marketing team are within the MarketingRG resource group. You need to provide access for Adam to manage all resources at the MarketingRG scope. Which of the following built-in roles would you assign to Adam to provide access to manage all resources in the MarketingRG resource group without providing Adam the ability to create role assignments for MarketingRG?

Resource Group Manager

Contributor

Selected

The Contributor role would be the best solution for providing Adam with the permissions to manage all resources in the MarketingRG resource group, without giving Adam the permissions to make role assignments.

Owner

User Access Administrator

QUESTION 22

You have two subscriptions named Subscription1 and Subscription2. You are logged into Azure using Azure PowerShell from Computer1. How can you identify which subscription you are currently viewing and then switch from one subscription to the other for the current session at Computer1?

AzShow-Context

Set-AzContext -SubscriptionName

Selected

In Az PowerShell 3.7.0, `Set-AzContext` sets the tenant, subscription, and environment for cmdlets to use in the current session.

Select-AzContext

Get-AzContext

Selected

In Az PowerShell 3.7.0, 'Get-AzContext' gets the metadata used to authenticate Azure Resource Manager requests.

QUESTION 42

You have an on-premises file server named **campusshare** that you are extending using Azure File Sync. You have already created a sync group in Azure File Sync. What steps do you need to take to finish extending your on-premises file server with Azure File Sync?

- Enable replication Selected

You do not enable replication on Azure File Sync when extending on-premises file servers.
- Create a Recovery Services vault
- Install Microsoft Monitoring agent
- Register the server

Registering the server is one of the steps for extending on-premises file servers using Azure File Sync.
- Install Azure File Sync agent Selected

Installing the Azure File Sync agent is one of the steps for extending on-premises file servers using Azure File Sync.
- Create a server endpoint in your sync group Selected

Creating a server endpoint in your sync group is a step for extending on-premises file servers using Azure File Sync.

QUESTION 2

The senior manager of your IT department has asked that you use Azure Storage to replace your on-premises storage solution. You currently store your data redundantly across 3 different host machines in an on-premises data center. You are in the process of creating the storage account and must select a redundancy option. Which of the following options would you select to match your current on-premises infrastructure redundancy levels?

Geo-redundant

Locally redundant storage

Selected

Locally redundant storage provide you with data redundancy storing your data as three copies across 3 host machines within a physical location. LRS would be the option to select to match your current on-premises environment.

Geo-zone-redundant storage

Zone-redundant storage

QUESTION 21

You have the following Azure storage accounts in your subscription: stor1 (BlockBlobStorage) stor2 (FileStorage) stor3 (StorageV2) Which of these storage accounts can be converted to read-access geo-redundant storage (RA-GRS) based on their storage account kind?

stor3

Selected

StorageV2 does support read-access geo-redundant storage (RA-GRS) and is able to be converted.

stor2

stor1 and stor2

stor1, stor2, and stor3

QUESTION 44

Subscription1 contains an Azure VM named VM1 with the following configuration:

- VM Size: Standard_D2s_v3
- Public IP Address: 52.173.36.55
- Resource Group: RG1
- Availability Zone: None
- Location: Japan East
- Disk Type: Standard HDD

What are two things you can do to reduce data loss and achieve a 99.9% SLA?

Place the VM in an availability zone

Selected

Once you have created the VM, the availability zone cannot be changed.

Change the disk type to Premium SSD

Selected

Virtual machines with Premium SSD disks qualify for the 99.9% connectivity SLA.

Create a Recovery Services vault and enable replication for VM1

Creating a Recovery Services vault will allow you to back up the VM to a different region and location. You will enable replication to ensure that VM data and settings are continually replicated to the backup location for simple recovery.

Move VM1 to a paired region

QUESTION 60

You have a subscription named Subscription1. You create a new Azure VM in your subscription named VM5 running Windows 2012 R2. You try to connect and login to VM5, but you get an error that says, "We couldn't connect to the remote PC. Make sure the PC is turned on and connected to the network, and that remote access is enabled." You have verified that VM5 is running and has been assigned a public IP address. What change do you need to make in order to successfully connect and log in to VM5?

- Add a rule to the network security group that will allow port 3389

Selected

A network security group (NSG) is designed to filter traffic to and from Azure resources, including Azure VMs. Allowing port 3389 from your machine to the Azure VM will address the connection issue.

- Access the VM from a computer that is in the same subnet
- Select *Reset password* from the VM blade
- Use Network Watcher for detailed connection tracing

QUESTION 59

You have a network security group (NSG) that is associated with a network interface that is attached to an Azure virtual machine named VM1 running Windows Server 2019. VM1 is in subnet named subnet1, in a virtual network named VNet1. A different NSG is attached to subnet1, but you notice that there is an inbound rule to allow port 3389. When you try to connect to VM1, you cannot connect. You reviewed the NSG and the source IP address and the protocol are correct. Which action should you take according to best practices for NSGs in Azure?

- The NSG attached to the network interface needs to be removed

Removing the NSG from the network interface would allow the VM to use the NSG associated with the subnet, which is best practice.

- An inbound rule for the NSG attached to the network interface needs to be added

Selected

NSGs attached to network interfaces are discouraged. This would solve the problem, but is redundant and unnecessary, as well as bad practice.

- The protocol on the NSG rule is set to UDP
- The source IP address on the NSG rule is incorrect

You have two subscriptions, one named Subscription1 and the other named Subscription2. Both subscriptions are located within the same tenant. You have one Azure virtual machine located within Subscription1 and another Azure virtual machine within Subscription2, and you'd like to view CPU utilization metrics on both virtual machines. How can you achieve this while maintaining the minimum number of Azure resources and minimizing cost?

Turn on VM insights in Azure Monitor

Selected

VM insights integration with Azure Monitor Logs delivers powerful aggregation and filtering, allowing Azure Monitor to analyze VM data trends over time. You can view this data in a single VM from the virtual machine directly, or you can use Azure Monitor to deliver an aggregated view of your VMs where the view supports Azure resource-context or workspace-context modes.

Create a Log Analytics workspace for both VMs

You can view metrics data (such as CPU utilization percentage) over time by sending your metrics data to a Log Analytics workspace. This workspace can collect metrics data from multiple VMs, no matter if they are located in the same or different subscriptions.

Enable guest-level monitoring on each VM

Selected

You do not need guest-level monitoring enabled on either VM to collect CPU metrics data. Enabling guest-level monitoring would not meet the requirement of this scenario in maintaining a minimum number of Azure resources at the lowest cost.

Install the Log Analytics agent on the VMs

QUESTION 5

You have a subscription named Subscription1. You would like to be alerted upon certain administrative events within Subscription1 to detect unauthorized access. Which of the following is the quickest method to set up these types of alerts?

Monitor > Alerts > New Alert Rule

Selected

Alerts can be created from within Azure Monitor.

Subscriptions > *mySubscription* > Activity Log > New Alert

Log Analytics Workspace > *myWorkspace* > Advanced Settings

Policy > Assignments > Assign Policy

QUESTION 28

You have a .NET Core application running in Azure App Services. You are expecting a huge influx of traffic to your application in the coming days. When your application experiences this spike in traffic, you want to detect any anomalies such as request errors or failed queries immediately. What service can you use to assure that you know about these types of errors related to your .NET application immediately?

- Search feature in Application Insights
- Client-side monitoring
- Log Analytics workspace
- Live Metrics Stream in Application InsightsSelected

Live Metrics Stream includes such information as the number of incoming requests, the duration of those requests, and any failures that occur. You can also inspect critical performance metrics such as processor and memory.

QUESTION 35

You have a number of virtual machines and web applications running in your Azure environment. These Azure resources are critical for business operations, so you've locked the resources in order to prevent deletion. In addition, how can you alert on these actions in the portal, and notify your team via email and SMS when a user is trying to delete or create a new resource from within your Azure subscription?

- Create a new action group

Selected

An action group is a collection of notification preferences defined by the owner of an Azure subscription. Azure Monitor and Service Health alerts use action groups to notify users that an alert has been triggered.

- Create a new alert rule

Selected

Alert rules specify the conditions for which the alert is triggered. Activity log alerts are the alerts that get activated when a new activity log event occurs that matches the conditions specified in the alert.

- Pin the activity log to your dashboard

- Query administrative events and copy link to query

  Rate this question

QUESTION 3

The following scenario will be the same for every question in this exam. Based on the information presented, please answer the question included below the scenario:

Axio Data Solutions is a big data company. They have offices in Seattle, London, and Tokyo with 500 Active Directory users at each location. The single domain forest is `axiodata.com` and has a domain functional level of Windows Server 2012. The company is making an effort to migrate their infrastructure to Azure cloud. They have just purchased an Azure subscription, as well as created their first Azure tenant.

In each of the three offices, there is a server room which consists of all the necessary infrastructure to host their directory, applications, and data. They do have a number of contractors that use their own devices. These devices are not connected to the network, and the Active Directory environment is not aware of these devices. These devices are used to access company data that may or may not be sensitive in nature.

After enforcing that all devices in use be registered with the domain, they have some problems joining the devices. During the domain join process, the device fails during authentication or the credentials fail during authorization. You have verified that the device is connected to the same network and responds when pinging the domain controller.

Axio Data Solutions plans to open a new office in Mumbai and hire 20 new people. In the next 6 months, all 20 users will be accessing all of their data and applications in Azure needed to perform their duties. They will use the same Active Directory environment, which will be synchronized with Azure AD. Also, users in Tokyo will need Azure Active Directory Seamless Single Sign-On (SSO) enabled.

Using the default route tables in Azure, they plan to create three virtual networks. The names of the virtual networks will be `Seattle-VNet`, `Contractor-VNet`, and `All-VNet`.

`Seattle-VNet` will contain two subnets named `Subnet1` and `Subnet2`. `Contractor-VNet` will contain two subnets named `Subnet3` and `Subnet4`. They plan to peer the virtual networks and enable remote gateways. Each subnet will contain a mix of Windows Server 2012 R2, Windows Server 2019, and RedHat Linux Server.

With web developers having full access to create Web Apps in Azure, Axio plans to deploy multiple web apps in a resource group named `web-rg` for each department. During this time, however, the Finance department must be able to monitor spending and control cost.

time, however, the finance department must be able to monitor spending and control cost.

Months after setting up the Mumbai office, you get a call from someone in Sales. They have to enter their password each time they access their customer relationship manager (CRM) application. How do you solve this problem?

- ✓ Ensure that their device is joined to the domain.
 - For Seamless SSO to function, you have to be using a device that is joined to the domain.
- ✓ Go to Azure Active Directory > Azure AD Connect and check the sign-in status of the user.
 - You can check the status of Seamless SSO by going to the Azure AD Connect pane.
- ✗ Run Azure AD Connect and uncheck **Enable single sign-on**.
 - This will disable Seamless SSO, which is not a part of the solution.
- ✗ Instruct the user to wait 30 minutes and try again.

time, however, the Finance department must be able to monitor spending and control cost.

After migrating to Azure, the web developers want to implement Application Insights for web apps. You have created an Application Insights resource in the same resource group as the web apps, so they can implement instrumentation into the apps. When trying to access the Application Insights resource, they receive a "Permissions denied" error. You want the developers to be able to use web tests and alerts with this resource. How do you fix this using the principle of least privilege?

- Assign the web developers the Global Administrator role
- Assign the web developers the Owner role at the scope of the resource group
- Assign the web developers the Contributor role at the scope of the resource group

You would assign the web developers the Contributor role to follow the principle of least privilege. Applying this role at the scope of the resource group will allow the web developers to use web tests and alerts on the Application Insights resource.

- Assign the web developers the Contributor role at the scope of the Application Insights resource Selected
- If you do this, the web developers will not be able to use web tests and alerts within the Application Insights resource.

When the accountants in the Finance department try to access the spending reports in the `web-rg` resource group, they are denied access. What do you need to do for them to view those spending reports?

- Assign them the Reader role for the subscription
- Assign them the Cost Management Reader role for the `web-rg` resource group

The Cost Management Reader role allows access to only billing components, such as Cost Management and Consumption.
- Assign them the Contributor role for Web Apps
- Assign them the Reader role for the `web-rg` resource group Selected

The Reader role will allow the user to view everything inside the resource group. There are other resources that the Finance department does not need to view.

After troubleshooting further, you realize that the SAMAccountName for one of the Active Directory users is too long. How should you go about fixing this?

- Change the name to less than 20 characters

Selected

This attribute must be 20 characters or less to support earlier clients, and cannot contain any of the following characters: `"/ \ [] : ; | = , + *`
`? < >`

- Enable Seamless Single Sign-On (SSO)
- Try to use another UPN when joining the device to the domain
- Wait for the synchronization process to complete, then try again

 Rate this question

In trying to ensure that users working on Azure virtual machines can connect to the on-premises servers, you run a trace route to the server, and you see a hop that is a public address outside of your network. What could be the reason for this?

- The two virtual networks are not peered together.
- The hop was to the gateway, since there is not a private connection like an ExpressRoute from this office to the on-premises location.
 - Since all locations are set up in a hub-and-spoke topology using a site-to-site VPN, all communication will go over the public internet.
- There is a custom route table in Azure that ensures that all traffic goes out of a network virtual appliance.
- The device that you are using to ping is a device that is not connected to the domain.

QUESTION 1

The following scenario will be the same for every question in this exam. Based on the information presented, please answer the question included below the scenario:

Consilium Care is a medical devices company that distributes to many hospitals around the globe. Consilium Care has a partner network that brings the devices to the market in each locale. The parts are made in China and assembled in Brussels. The assembly process includes many diverse sets of instructions to fit together the thousands of pieces it takes to make any one instrument. The sub-assembly and assembly teams keep their documents, instructions, and parts in various servers throughout the datacenter. Consilium Care's environment consists of file servers, SQL servers, and domain controllers. The single forest domain, consiliumcaregroup.com, consists of over 2,000 servers and devices all joined to the domain.

Their inventory management system is managed via an application with a SQL backend, a web frontend, and middleware. Users access the web frontend over SSL (HTTPS) only. Consilium Care plans to move this application to Azure, while also moving all documents and instruction files to Azure Blob storage. This migration includes moving all virtual machines to Azure, copying all files over the internet to Blob storage, and ensuring all access to Azure resources is secure, including access to storage.

Taking advantage of identity control in Azure, Consilium Care wants every user to use multi-factor authentication and to verify their identity using their phone or email. Also, only a certain group can add devices to the domain. Finally, only one user should be able to add and remove resources from the Azure subscription.

Consilium Care is concerned about data security. Now that they have all of their infrastructure in Azure, they realize the potential attack vectors. They have lots of private documents and patents, so they need to secure these files, which primarily reside on Windows Server 2012 R2 Core. What items might they need to install to configure disk encryption on their boot drives and data drives?

- Azure Disk Encryption Selected
 - Azure Disk Encryption for Windows VMs provides disk encryption and helps manage the encryption keys and secrets used to securely access your data.
- Bitlocker Selected
 - The Bitlocker feature is included with Windows to provide volume-level encryption for the OS and the data disks. Since this is a built-in feature, they won't need to install it.
- Azure Key Vault Selected
 - Azure Key Vault provides and stores the encryption keys and secrets necessary to access your encrypted disks.
- Azure Monitor
- bdehdcfg component
 - Windows Server 2012 R2 Core and Windows Server 2016 Core requires the bdehdcfg component to be installed on the VM for encryption.

You have successfully moved all virtual machines to Azure. You realize that having a backup of these servers is extremely important. You would like the ability to restore the entire VM and individual files and folders, but also delete backup data instantly if needed. What do you need to do in Azure to meet these requirements?

- Create a Recovery Services vault

Selected

You will need a Recovery Services vault to store the backup data for a VM in Azure.

- Disable soft-delete

Soft-delete is a feature that is turned on by default and protects against accidental deletion. Disabling this feature allows you to delete backup data immediately when you stop the backup.

- Replicate the VM to a different region

- Create a backup policy

Selected

You will need a backup policy to configure the frequency and retention of VM backups.

- Create a Site Recovery policy

Selected

A Site Recovery policy is for when you experience entire site outages, and allows for failover to a secondary site. This is above and beyond the requirement for this scenario.

You've finished setting up access control for the user that is able to add and remove resources within the Azure subscription. Additionally, you would like to set up an alert to notify them when regional outages occur. What do you do?

Monitor > Alerts > New Alert Rule

Selected

Creating a new alert rule will not satisfy this requirement, as this is a service event, which is outside the scope of your current subscription.

Monitor > Alerts > Manage Actions > Add Action Group

Selected

In order to notify the user via email or SMS, you must create an action group.

Service Health > Service Issues > Add Service Health Alert

A Service Health Alert is an event tracking tool in Azure. You can track active events like ongoing service issues, upcoming planned maintenance, or relevant health advisories.

Subscriptions > *mySubscription* > Access Control

In order to move the files to Azure Blob storage, and keeping in mind the requirement during the migration described above, which method should you use?

Order an Azure Data Box and transfer the files to it.

Map an Azure file share to your Windows 10 laptop and use Windows File Explorer to copy the files.

Ship the drives to Microsoft using the Import/Export service.

Selected

The requirement outlined in the scenario was to copy the files over the internet, and this option does not meet that requirement.

Use Storage Explorer to copy the files.

Storage Explorer is an efficient, fast, and secure way to copy data to Azure blobs. Storage Explorer also lets you work disconnected from the cloud or offline with local emulators.

The engineers responsible for the frontend of the application want monitoring capabilities. They want to not only monitor uptime and traffic to the application, but they also want to measure performance counters and perform diagnostics on the underlying VM. What Azure features would you recommend?

Application Insights

Selected

Application Insights can be used for App Services Apps in Azure and even in on-premises VMs.

SQL Analytics

Azure Virtual Machine Scale Sets

VM Insights (Azure Monitor for VMs)

Selected

VM Insights (also known as Azure Monitor for VMs) monitors your Azure virtual machines and virtual machine scale sets at scale. It analyzes the performance and health of your Windows and Linux VMs, and monitors their processes and dependencies on other resources and external processes. It includes support for monitoring performance and application dependencies for VMs that are hosted on-premises or in another cloud provider.