

Virtual machines in Azure	Proximity Placement Groups are a grouping construct used to ensure Azure compute resources are physically located close to each other. Proximity placement groups are useful for workloads where low latency is a requirement.																					
Managed Disks	Managed Disks handles Azure Storage account creation and management in the background for you, and ensures that you do not have to worry about the scalability limits of the storage account. You specify the disk size and the performance tier (Standard or Premium), and Azure creates and manages the disk.																					
VM Sizes Compute / Memory / Storage Optimized General Purpose / GPU / High Performance Compute (Checkout the sizes available while creating a VM)	<table><tr><th>Type</th><th>Sizes</th><th>Description</th></tr><tr><td>General purpose</td><td>B, Dsv3, Dv3, Dasv4, Dav4, DSv2, Dv2, Av2, DC, DCv2, Dpdsv5, Dpldsv5, Dpsv5, Dplsv5, Dv4, Dsv4, Ddv4, Ddsdv4, Dv5, Dsv5, Ddv5, Ddsdv5, Dasv5, Dadsv5</td><td>Balanced CPU-to-memory ratio. Ideal for testing and development, small to medium databases, and low to medium traffic web servers.</td></tr><tr><td>Compute optimized</td><td>F, Fs, Fsv2, FX</td><td>High CPU-to-memory ratio. Good for medium traffic web servers, network appliances, batch processes, and application servers.</td></tr><tr><td>Memory optimized</td><td>Esv3, Ev3, Easv4, Eav4, Epdsv5, Epsv5, Ev4, Esv4, Edv4, Edsv4, Ev5, Esv5, Edv5, Edsv5, Easv5, Eadsv5, Mv2, M, DSv2, Dv2</td><td>High memory-to-CPU ratio. Great for relational database servers, medium to large caches, and in-memory analytics.</td></tr><tr><td>Storage optimized</td><td>Lsv2, Lsv3, Lasv3</td><td>High disk throughput and IO ideal for Big Data, SQL, NoSQL databases, data warehousing and large transactional databases.</td></tr><tr><td>GPU</td><td>NC, NCv2, NCv3, NCasT4_v3, ND, NDv2, NV, NVv3, NVv4, NDasrA100_v4, NDm_A100_v4</td><td>Specialized virtual machines targeted for heavy graphic rendering and video editing, as well as model training and inferencing (ND) with deep learning. Available with single or multiple GPUs.</td></tr><tr><td>High performance compute</td><td>HB, HBv2, HBv3, HC, H</td><td>Our fastest and most powerful CPU virtual machines with optional high-throughput network interfaces (RDMA).</td></tr></table> General purpose virtual machine sizes	Type	Sizes	Description	General purpose	B, Dsv3, Dv3, Dasv4, Dav4, DSv2, Dv2, Av2, DC, DCv2, Dpdsv5, Dpldsv5, Dpsv5, Dplsv5, Dv4, Dsv4, Ddv4, Ddsdv4, Dv5, Dsv5, Ddv5, Ddsdv5, Dasv5, Dadsv5	Balanced CPU-to-memory ratio. Ideal for testing and development, small to medium databases, and low to medium traffic web servers.	Compute optimized	F, Fs, Fsv2, FX	High CPU-to-memory ratio. Good for medium traffic web servers, network appliances, batch processes, and application servers.	Memory optimized	Esv3, Ev3, Easv4, Eav4, Epdsv5, Epsv5, Ev4, Esv4, Edv4, Edsv4, Ev5, Esv5, Edv5, Edsv5, Easv5, Eadsv5, Mv2, M, DSv2, Dv2	High memory-to-CPU ratio. Great for relational database servers, medium to large caches, and in-memory analytics.	Storage optimized	Lsv2, Lsv3, Lasv3	High disk throughput and IO ideal for Big Data, SQL, NoSQL databases, data warehousing and large transactional databases.	GPU	NC, NCv2, NCv3, NCasT4_v3, ND, NDv2, NV, NVv3, NVv4, NDasrA100_v4, NDm_A100_v4	Specialized virtual machines targeted for heavy graphic rendering and video editing, as well as model training and inferencing (ND) with deep learning. Available with single or multiple GPUs.	High performance compute	HB, HBv2, HBv3, HC, H	Our fastest and most powerful CPU virtual machines with optional high-throughput network interfaces (RDMA).
Type	Sizes	Description																				
General purpose	B, Dsv3, Dv3, Dasv4, Dav4, DSv2, Dv2, Av2, DC, DCv2, Dpdsv5, Dpldsv5, Dpsv5, Dplsv5, Dv4, Dsv4, Ddv4, Ddsdv4, Dv5, Dsv5, Ddv5, Ddsdv5, Dasv5, Dadsv5	Balanced CPU-to-memory ratio. Ideal for testing and development, small to medium databases, and low to medium traffic web servers.																				
Compute optimized	F, Fs, Fsv2, FX	High CPU-to-memory ratio. Good for medium traffic web servers, network appliances, batch processes, and application servers.																				
Memory optimized	Esv3, Ev3, Easv4, Eav4, Epdsv5, Epsv5, Ev4, Esv4, Edv4, Edsv4, Ev5, Esv5, Edv5, Edsv5, Easv5, Eadsv5, Mv2, M, DSv2, Dv2	High memory-to-CPU ratio. Great for relational database servers, medium to large caches, and in-memory analytics.																				
Storage optimized	Lsv2, Lsv3, Lasv3	High disk throughput and IO ideal for Big Data, SQL, NoSQL databases, data warehousing and large transactional databases.																				
GPU	NC, NCv2, NCv3, NCasT4_v3, ND, NDv2, NV, NVv3, NVv4, NDasrA100_v4, NDm_A100_v4	Specialized virtual machines targeted for heavy graphic rendering and video editing, as well as model training and inferencing (ND) with deep learning. Available with single or multiple GPUs.																				
High performance compute	HB, HBv2, HBv3, HC, H	Our fastest and most powerful CPU virtual machines with optional high-throughput network interfaces (RDMA).																				

	<p>General purpose VM sizes provide balanced CPU-to-memory ratio. Ideal for testing and development, small to medium databases, and low to medium traffic web servers. This article provides information about the offerings for general purpose computing.</p> <p>Compute optimized virtual machine sizes</p> <p>Compute optimized VM sizes have a high CPU-to-memory ratio. These sizes are good for medium traffic web servers, network appliances, batch processes, and application servers. This article provides information about the number of vCPUs, data disks, and NICs. It also includes information about storage throughput and network bandwidth for each size in this grouping.</p> <p>Memory optimized virtual machine sizes</p> <p>Memory optimized VM sizes offer a high memory-to-CPU ratio that is great for relational database servers, medium to large caches, and in-memory analytics. This article provides information about the number of vCPUs, data disks and NICs. You can also learn about storage throughput and network bandwidth for each size in this grouping.</p> <p>Storage optimized virtual machine sizes</p> <p>Storage optimized virtual machine (VM) sizes offer high disk throughput and IO, and are ideal for Big Data, SQL, NoSQL databases, data warehousing, and large transactional databases. Examples include Cassandra, MongoDB, Cloudera, and Redis. This article provides information about the number of vCPUs, data disks, NICs, local storage throughput, and network bandwidth for each optimized size.</p> <p>GPU optimized virtual machine sizes</p> <p>GPU optimized VM sizes are specialized virtual machines available with single, multiple, or fractional GPUs. These sizes are designed for compute-intensive, graphics-intensive, and visualization workloads. This article provides information about the number and type of GPUs, vCPUs, data disks, and NICs. Storage throughput and network bandwidth are also included for each size in this grouping.</p> <p>High performance computing VM sizes</p> <p>Azure H-series virtual machines (VMs) are designed to deliver leadership-class performance, scalability, and cost efficiency for various real-world HPC workloads.</p>
VM Power states and billing	Creating → Starting → Running (Stopping → Stopped or Deallocating → Deallocated)

Power state	Description	Billing
Creating	Virtual machine is allocating resources.	Not Billed*
Starting	Virtual machine is powering up.	Billed
Running	Virtual machine is fully up. This state is the standard working state.	Billed
Stopping	This state is transitional between running and stopped.	Billed
Stopped	The virtual machine is allocated on a host but not running. Also called <i>PoweredOff</i> state or <i>Stopped (Allocated)</i> . This state can be result of invoking the <code>PowerOff</code> API operation or invoking shutdown from within the guest OS. The <i>Stopped</i> state may also be observed briefly during VM creation or while starting a VM from <i>Deallocated</i> state.	Billed
Deallocating	This state is transitional between <i>Running</i> and <i>Deallocated</i> .	Not billed*
Deallocated	The virtual machine has released the lease on the underlying hardware and is powered off. This state is also referred to as <i>Stopped (Deallocated)</i> .	Not billed*

Azure compute gallery

An Azure Compute Gallery helps you build structure and organization around your Azure resources, like images and [applications](#).

Scaling (Create Azure Compute Gallery, checkout no. of replicas)	<p>Azure Compute Gallery allows you to specify the number of replicas you want to keep. This helps in multi-VM deployment scenarios as the VM deployments can be spread to different replicas reducing the chance of instance creation processing being throttled due to overloading of a single replica.</p> <ul style="list-style-type: none">For every 20 VMs that you create concurrently, we recommend you keep one replica. For example, if you are creating 120 VMs concurrently using the same image in a region, we suggest you keep at least 6 replicas of your image.
--	--

	<ul style="list-style-type: none">For each scale set you create concurrently, we recommend you keep one replica.								
High availability (check HA option)	<p>Azure Zone Redundant Storage (ZRS) provides resilience against an Availability Zone failure in the region. With the general availability of Azure Compute Gallery, you can choose to store your images in ZRS accounts in regions with Availability Zones.</p> <p>You can also choose the account type for each of the target regions. The default storage account type is Standard_LRS, but you can choose Standard_ZRS for regions with Availability Zones. For more information on regional availability of ZRS, see Data redundancy.</p>								
Replication (Check replication options)	Azure Compute Gallery also allows you to replicate your resources to other Azure regions automatically. Each image version can be replicated to different regions depending on what makes sense for your organization.								
Sharing	<table><tr><th>Share with:</th><th>Option</th></tr><tr><td>Specific people, groups, or service principals</td><td>Role-based access control (RBAC) lets you share resources to specific people, groups, or service principals on a granular level.</td></tr><tr><td>Subscriptions or tenants</td><td>Direct shared gallery (preview) lets you share to everyone in a subscription or tenant.</td></tr><tr><td>Everyone</td><td>Community gallery (preview) lets you share your entire gallery publicly, to all Azure users.</td></tr></table>	Share with:	Option	Specific people, groups, or service principals	Role-based access control (RBAC) lets you share resources to specific people, groups, or service principals on a granular level.	Subscriptions or tenants	Direct shared gallery (preview) lets you share to everyone in a subscription or tenant.	Everyone	Community gallery (preview) lets you share your entire gallery publicly, to all Azure users.
Share with:	Option								
Specific people, groups, or service principals	Role-based access control (RBAC) lets you share resources to specific people, groups, or service principals on a granular level.								
Subscriptions or tenants	Direct shared gallery (preview) lets you share to everyone in a subscription or tenant.								
Everyone	Community gallery (preview) lets you share your entire gallery publicly, to all Azure users.								
Create a gallery for storing and sharing resources	<p>Azure compute gallery create:</p> <ol style="list-style-type: none">Basics: Specify nameSharing: Specify sharing method								

Basics Sharing Tags Review + create

Azure compute galleries allow you to share images with users or user groups. Images are published to an Azure compute gallery that will be available within your subscription. [Learn more about Azure compute galleries](#)

Project details

Select the subscription to manage deployed resources and costs. Use the resource group to manage your resources.

Subscription * ⓘ

Pay-As-You-Go

Resource group * ⓘ

computegalrg

Create new

Instance details

Name * ⓘ

mynewgal

Region * ⓘ

(US) East US

Description ⓘ

Basics **Sharing** Tags Review + create

In addition to role based sharing through Identity Access control, you're able to share the compute gallery using the methods below.

Sharing method ⓘ

☒ Role based access control (RBAC)

Role based sharing through Identity Access control. Share based on permissions assigned to users, groups, and applications at a certain scope. [Learn more](#)

☐ RBAC + share directly (Preview)

Share resources with all users in the same subscription, same tenant, different subscriptions, and different tenants. All users in the subscription or tenant will have read access to the gallery and all the resources within it. [Learn more](#)

☐ RBAC + share to public community gallery (PREVIEW)

Publish your Azure compute gallery to the community gallery. Your gallery will be shared with anyone using Azure, including users outside of your organization. [Learn more](#)

- ⚠

This subscription is not registered with the feature Microsoft.Compute/DirectSharedGalleries. Please register the subscription to directly share galleries across subscriptions and tenants.
- ⚠

This subscription is not registered with the feature Microsoft.Compute/CommunityGalleries. Please register the subscription for sharing to public community gallery.

Store and share images in an Azure Compute Gallery

(create image definitions, and image version)

When you use a gallery to store images, multiple resource types are created:







Resource	Description
Image source	This is a resource that can be used to create an image version in a gallery. An image source can be an existing Azure VM that is either generalized or specialized , a managed image, a snapshot, a VHD or an image version in another gallery.
Gallery	Like the Azure Marketplace, a gallery is a repository for managing and sharing images and other resources, but you control who has access.
Image definition	Image definitions are created within a gallery and they carry information about the image and any requirements for using it to create VMs. This includes whether the image is Windows or Linux, release notes, and minimum and maximum memory requirements. It is a definition of a type of image.
Image version	An image version is what you use to create a VM when using a gallery. You can have multiple versions of an image as needed for your environment. Like a managed image, when you use an image version to create a VM, the image version is used to create new disks for the VM. Image versions can be used multiple times.

Image definitions




Image definitions are a logical grouping for versions of an image. The image definition holds information about why the image was created, what OS it is for, and other information about using the image. You don't deploy a VM from an image definition, but from the image versions created from the definition.

Go to Gallery >> Add Image Definition.

«

-  Overview
-  Activity log
-  Access control (IAM)
-  Tags
-  Diagnose and solve problems
-  Settings

 Add ▾  Delete  Refresh

-  VM image definition
-  VM application definition 

Location [\(move\)](#) : East US

Subscription [\(move\)](#) : Pay-As-You-Go

Subscription ID : bbbf29b6-54bc-46d2-89ad-7d0f46

Status : Succeeded

While creating Image Definitions you need to specify **def name, OS type, Generations, Publisher name(MicrosoftWindowsServer), Offer(WindowsServer), SKU(2019-Datacenter)**

Basics Version Publishing options Tags Review + create

Images are defined within a gallery and carry information about the image and requirements for using it internally. This includes whether the image is Windows or Linux, release notes, and minimum and maximum memory requirements.
[Learn more about VM image definitions](#)

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription ⓘ	<div>Pay-As-You-Go</div>
Resource group ⓘ	<div>computegalrg</div>

Instance details

Region * ⓘ	<div>(Asia Pacific) Central India</div>
------------	---

VM image definition details

Target Azure compute gallery ⓘ	<div>computegal</div>
--------------------------------	-----------------------

VM image definition name * ⓘ	<div></div>
------------------------------	-------------

OS type * ⓘ	<div><div><input checked="" type="radio"/> Windows</div><div><input type="radio"/> Linux</div></div>
-------------	--

Security type ⓘ	<div>Standard</div>
-----------------	---------------------

VM generation * ⓘ	<div><div><input checked="" type="radio"/> Gen 1</div><div><input type="radio"/> Gen 2</div></div>
-------------------	--

Higher storage performance with NVMe (preview) ⓘ	<div><input type="checkbox"/></div> <div><div> NVMe is not registered for the selected subscription.</div></div>
--	--

OS state * ⓘ	<div><div><input checked="" type="radio"/> Generalized</div><div><input type="radio"/> Specialized</div></div>
--------------	--

VM architecture ⓘ	<div><div><input checked="" type="radio"/> x64</div><div><input type="radio"/> Arm64</div></div> <div><div> Arm64 VM architecture is not supported with generation 1 virtual machines.</div></div>
-------------------	--

Publisher * ⓘ	<div></div>
---------------	-------------

Offer * ⓘ	<div></div>
-----------	-------------


SKU * ⓘ	<div></div>
---------	-------------

Image versions

An image version is what you use to create a VM. You can have multiple versions of an image as needed for your environment. When you use an image version to create a VM, the image version is used to create new disks for the VM. Image versions can be used multiple times.

Go to Image def >> Add version

[Home](#) > [Azure compute galleries](#) > [computegal](#) >

 **mydef (computegal/mydef)** ☆ ...

VM image definition

«

+ Add version

+ Create VM

Overview

Activity log

Access control (IAM)

^ Essentials

Resource group (move) : computega

Location (move) : East US

While creating the image version you need to specify version no, source and source image under Basics tab.

Basics

Replication

Encryption

Tags

Review + create

Create a new image that can be used to deploy virtual machines and virtual machine scale sets. With a shared image, you can easily replicate the image to Azure regions around the world and manage versions of the image. [Learn more](#)

Project details

Subscription ⓘ

Pay-As-You-Go

Resource group ⓘ

computegalrg

Instance details

Region * ⓘ

(US) East US

Version details

Version number * ⓘ

Example: 0.0.1, 15.35.0

Source * ⓘ

Managed image

Source image * ⓘ

Disks and/or snapshots

VM image version

Managed image

Storage blobs (VHDs)

Exclude from latest ⓘ

End of life date ⓘ

Replication:

The default storage sku to be used for the image per region.

The default number of replicas to be created per region. The default value can be overridden per region in the replication table.

Basics **Replication** Encryption Tags Review + create

A VM image version can be replicated to different regions depending on what makes sense for your organization. One example is to always replicate the latest image in multiple regions while all older versions are only available in 1 region. This can help save on storage costs for VM image versions. [Learn more](#)

Replication

Default storage sku ⓘ
Default replica count * ⓘ

Target regions

(US) East US

1

Zone-redundant

(US) West US 3

1

Standard HDD LRS

(Asia Pacific) Central India

1

Standard HDD LRS

1

Zone-redundant

Generalized and specialized images

There are two operating system states supported by Azure Compute Gallery. Typically images require that the VM used to create the image has been **generalized** before taking the image. Generalizing is a process that removes machine and user specific information from the VM. For Linux, you can use `waagent -deprovision` or `-deprovision+user` parameters. For Windows, the Sysprep tool is used.

Shallow replication

	<p>When you create an image version, you can set the replication mode to shallow for development and test. Shallow replication skips copying the image, so the image version is ready much faster. But, it also means you can't deploy a large number of VMs from that image version. This is similar to the way that the older managed images worked.</p>
Use customer-managed keys for encrypting images	<p>Images in an Azure Compute Gallery (formerly known as Shared Image Gallery) are stored as snapshots, so they're automatically encrypted through server-side encryption.</p> <p>You can rely on platform-managed keys for the encryption of your images, or use your own keys. You can also use both together, for double encryption. If you choose to manage encryption with your own keys, you can specify a <i>customer-managed</i> key to use for encrypting and decrypting all disks in your images.</p> <p>Limitations</p> <ul style="list-style-type: none"> • Encryption key sets must be in the same subscription as your image. • Encryption key sets are regional resources, so each region requires a different encryption key set. • You can't copy or share images that use customer-managed keys. • After you've used your own keys to encrypt a disk or image, you can't go back to using platform-managed keys for encrypting those disks or images.
VM Applications overview (create an application and use it in VM setup)	<p>VM Applications are a resource type in Azure Compute Gallery (formerly known as Shared Image Gallery) that simplifies management, sharing, and global distribution of applications for your virtual machines.</p> <p>While you can create an image of a VM with apps pre-installed, you would need to update your image each time you have application changes. Separating your application installation from your VM images means there's no need to publish a new image for every line of code change.</p>
Bringing and creating Linux images in Azure (create a managed image)	<p>When bringing your Linux image you have two options:</p> <ul style="list-style-type: none"> • Managed images for simple VM creation in a development and test environment. • Azure Compute Gallery for creating and sharing images at-scale.

	<p>Managed images</p> <p>Managed images can be used to create multiple VMs, but they have a lot of limitations. Managed images can only be created from a generalized source (VM or VHD). They can only be used to create VMs in the same region and they can't be shared across subscriptions and tenants.</p> <p>Azure Compute Gallery</p> <p>Azure Compute Gallery (formerly known as Shared Image Gallery) is recommended for creating, managing, and sharing images at scale. Azure Compute Gallery helps you build structure and organization around your images.</p> <ul style="list-style-type: none">• Support for both generalized and specialized images.• Support for image both generation 1 and 2 images.• Global replication of images.• Versioning and grouping of images for easier management.• Highly available images with Zone Redundant Storage (ZRS) in regions that support Availability Zones. ZRS offers better resilience against zonal failures.• Sharing across subscriptions and even between Active Directory (AD) tenants using Azure RBAC.• Scaling your deployments with image replicas in each region. <p>At a high level, you create a gallery and it is made up of:</p> <ul style="list-style-type: none">• Image Definitions - These are containers that hold groups of images.• Image Versions - These are the actual images.
<h2>Azure Dedicated Hosts</h2>	
	<p>Azure Dedicated Host is a service that provides physical servers - able to host one or more virtual machines - dedicated to one Azure subscription.</p>
Groups, hosts, and VMs (host group create/dedicated server create)	<p>A host group is a resource that represents a collection of dedicated hosts. You create a host group in a region and an availability zone, and add hosts to it.</p>

	<p>A host is a resource, mapped to a physical server in an Azure data center. The physical server is allocated when the host is created. A host is created within a host group. A host has a SKU describing which VM sizes can be created. Each host can host multiple VMs, of different sizes, as long as they are from the same size series.</p>
Manual vs. automatic placement	<p>When creating a VM in Azure, you can select which dedicated host to use. You can also use the option to automatically place your VMs on existing hosts, within a host group.</p> <p>When creating a new host group, make sure the setting for automatic VM placement is selected. When creating your VM, select the host group and let Azure pick the best host for your VM.</p>
<h2>Azure Spot Virtual Machines</h2>	
	<p>Using Azure Spot Virtual Machines allows you to take advantage of our unused capacity at a significant cost savings. At any point in time when Azure needs the capacity back, the Azure infrastructure will evict Azure Spot Virtual Machines. Therefore, Azure Spot Virtual Machines are great for workloads that can handle interruptions like batch processing jobs, dev/test environments, large compute workloads, and more.</p> <p>VMs can be evicted based on capacity or the max price you set. When creating an Azure Spot Virtual Machine, you can set the eviction policy to <i>Deallocate</i> (default) or <i>Delete</i>.</p>
<h2>Azure Reservations</h2> <ul style="list-style-type: none">• Reserved Instances• On demand capacity reservation	
(create reserved instance)	<p>Azure Reservations help you save money by committing to one-year or three-year plans for multiple products. Committing allows you to get a discount on the resources you use. Reservations can significantly reduce your resource costs by up to 72% from pay-as-you-go prices. Reservations provide a billing discount and don't affect the runtime state of your resources. After you purchase a reservation, the discount automatically applies to matching resources.</p> <p>You can pay for a reservation up front or monthly. The total cost of up-front and monthly reservations is the same and you don't pay any extra fees when you choose to pay monthly.</p>

On demand capacity reservation (create on demand capacity reservation)

On-demand Capacity Reservation enables you to reserve Compute capacity in an Azure region or an Availability Zone for any duration of time. Unlike [Reserved Instances](#), you do not have to sign up for a 1-year or a 3-year term commitment.

Once Azure accepts a reservation request, it is available to be consumed by VMs of matching configurations. To consume Capacity Reservation, the VM will have to specify the reservation as one of its properties. Otherwise, the Capacity Reservation will remain unused. One benefit of this design is that you can target only critical workloads to reservations and other non-critical workloads can run without reserved capacity.

Benefits of Capacity Reservation

- Once deployed, capacity is reserved for your use and always available within the scope of applicable SLAs
- Can be deployed and deleted at any time with no term commitment
- Can be combined automatically with Reserved Instances to use term commitment discounts

Difference between On-demand Capacity Reservation and Reserved Instances

Differences	On-demand Capacity Reservation	Reserved Instances
Term	No term commitment required. Can be created and deleted as per the customer requirement	Fixed term commitment of either one-year or three-years
Billing discount	Charged at pay-as-you-go rates for the underlying VM size*	Significant cost savings over pay-as-you-go rates
Capacity SLA	Provides capacity guarantee in the specified location (region or availability zone)	Does not provide a capacity guarantee. Customers can choose "capacity priority" to gain better access, but that option does not carry an SLA
Region vs Availability Zones	Can be deployed per region or per availability zone	Only available at regional level

Azure virtual machine extensions and features

Extensions are small applications that provide post-deployment configuration and automation on Azure VMs.

Virtual machine extensions and features for Linux

Azure CLI

```
az vm extension image list --location westus --output table
```

The following troubleshooting actions apply to all VM extensions:

- To check the Azure Linux Agent log, look at the activity when your extension was being provisioned in `/var/log/waagent.log`.
- Check the extension logs for more details in `/var/log/azure/<extensionName>`.
- Check troubleshooting sections in extension-specific documentation for error codes, known issues, and other extension-specific information.
- Look at the system logs. Check for other operations that might have interfered with the extension, such as a long-running installation of another application that required exclusive access to the package manager.

Diff extensions available for VMs

Azure Disk Encryption for Linux (Microsoft.Azure.Security.AzureDiskEncryptionForLinux)

Azure Disk Encryption leverages the dm-crypt subsystem in Linux to provide full disk encryption on [select Azure Linux distributions](#). This solution is integrated with Azure Key Vault to manage disk encryption keys and secrets.

Key Vault virtual machine extension for Linux

The Key Vault VM extension provides automatic refresh of certificates stored in an Azure key vault. Specifically, the extension monitors a list of observed certificates stored in key vaults. The extension retrieves and installs the corresponding certificates after detecting a change.

Use the Azure Custom Script Extension Version 2 with Linux virtual machines

The Custom Script Extension Version 2 downloads and runs scripts on Azure virtual machines (VMs). This extension is useful for post-deployment configuration, software installation, or any other configuration or management task.

Microsoft Antimalware Extension for Windows

	<p>VM Snapshot Linux extension for Azure Backup</p> <p>Network Watcher Agent virtual machine extension for Linux</p> <p>Azure Desired State Configuration extension handler</p> <p>VMAccess Extension with the Azure CLI: Manage administrative users, SSH, and check or repair disks on Linux VMs</p>
<h2>Availability and scale</h2>	
Availability options for Azure Virtual Machines	<ul style="list-style-type: none">• Availability zones• Virtual Machines Scale Sets• Availability sets: 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 recommended 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.• Load balancer• Azure Storage redundancy: Azure Storage always stores multiple copies of your data so that it is protected from planned and unplanned events, including transient hardware failures, network or power outages, and massive natural disasters.• Azure Site Recovery
Virtual Machines Scale Sets	<p>Orchestration modes for virtual machine scale sets in Azure:</p> <ul style="list-style-type: none">• Uniform orchestration:• Flexible orchestration:
Proximity placement groups	<p>A proximity placement group is a logical grouping used to make sure that Azure compute resources are physically located close to each other. Proximity placement groups are useful for workloads where low latency is a requirement.</p>
Region pairs	<p>Each Azure region is paired with another region within the same geography (such as US, Europe, or Asia).</p> <ul style="list-style-type: none">• In the event of a wider Azure outage, one region is prioritized out of every pair to help reduce the time to restore for applications.

	<ul style="list-style-type: none">Planned Azure updates are rolled out to paired regions one at a time to minimize downtime and risk of application outage.Data continues to reside within the same geography as its pair. <table><tr><th>Primary</th><th>Secondary</th></tr><tr><td>West US</td><td>East US</td></tr><tr><td>North Europe</td><td>West Europe</td></tr><tr><td>Southeast Asia</td><td>East Asia</td></tr></table>	Primary	Secondary	West US	East US	North Europe	West Europe	Southeast Asia	East Asia
Primary	Secondary								
West US	East US								
North Europe	West Europe								
Southeast Asia	East Asia								
Availability sets	<p>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 recommended 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.</p> <p>Each virtual machine in your availability set is assigned an update domain and a fault domain by the underlying Azure platform. Each availability set can be configured with up to three fault domains and twenty update domains. These configurations can't be changed once the availability set has been created.</p> <p>Update domains indicate groups of virtual machines and underlying physical hardware that can be rebooted at the same time. Only one update domain is rebooted at a time.</p> <p>Fault domains define the group of virtual machines that share a common power source and network switch.</p>								
Disks									
Types of managed disks	<p>The available types of disks are ultra disks, premium solid-state drives (SSD), standard SSDs, and standard hard disk drives (HDD).</p>								

	Ultra disk	Premium SSD v2	Premium SSD	Standard SSD	Standard HDD
Disk type	SSD	SSD	SSD	SSD	HDD
Scenario	IO-intensive workloads such as SAP HANA , top tier databases (for example, SQL, Oracle), and other transaction-heavy workloads.	Production and performance-sensitive workloads that consistently require low latency and high IOPS and throughput	Production and performance sensitive workloads	Web servers, lightly used enterprise applications and dev/test	Backup, non-critical, infrequent access
Max disk size	65,536 gibibyte (GiB)	65,536 GiB	32,767 GiB	32,767 GiB	32,767 GiB
Max throughput	4,000 MB/s	1,200 MB/s	900 MB/s	750 MB/s	500 MB/s
Max IOPS	160,000	80,000	20,000	6,000	2,000
Usable as OS Disk?	No	No	Yes	Yes	Yes

Ultra disk:

Ultra disks are suited for data-intensive workloads such as SAP HANA, top-tier databases, and transaction-heavy workloads. Ultra disks support IOPS limits of **300 IOPS/GiB, up to a maximum of 160,000 IOPS per disk. Ultra disks can't be used as OS disks, they can only be created as empty data disks.** Ultra disks also can't be used with some features and functionality, including disk export, disk snapshots, changing disk type, VM images, availability sets, or Azure disk encryption.

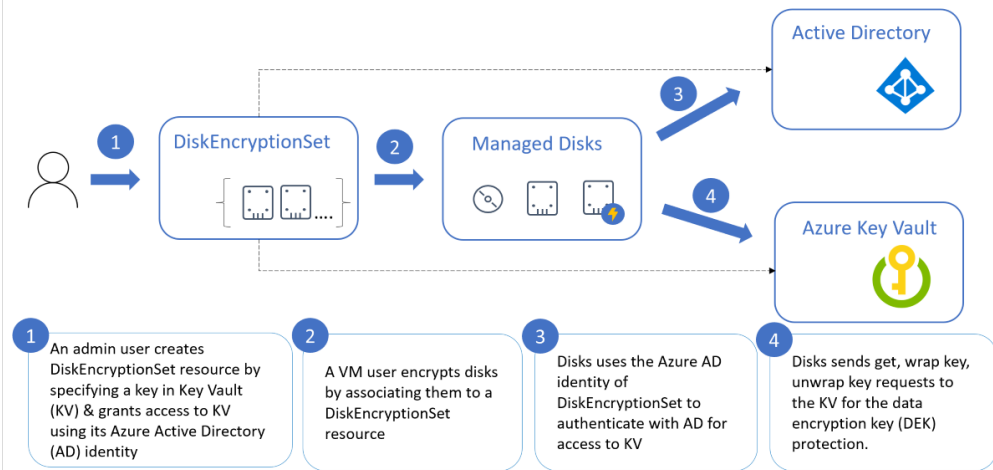
Premium SSD v2:

Premium SSD v2 is suited for a broad range of workloads such as **SQL server, Oracle, MariaDB, SAP, Cassandra, MongoDB, big data/analytics, and gaming, on virtual machines or stateful containers.** Premium SSD v2 disks can't be used as an OS disk. taking snapshots aren't supported,Azure Disk Encryption isn't supported. All Premium SSD v2 disks have a baseline IOPS of 3000 that is free of charge. After 6 GiB, the maximum IOPS a disk can have increases at a rate of 500 per GiB, up to **80,000 IOPS.**

Redundancy options for managed disks	<p>Azure managed disks offer two storage redundancy options,locally-redundant storage(LRS) and zone-redundant storage (ZRS).</p> <p>LRS: replicates your data three times within a single data center in the selected region. LRS protects your data against server rack and drive failures.</p> <p>ZRS: synchronously replicates your Azure managed disk across three Azure availability zones in the region you select.</p>
Overview of managed disk encryption options	<p>There are several types of encryption available for your managed disks, including</p> <p>Azure Disk Encryption (ADE),</p> <p>Server-Side Encryption (SSE) and</p> <p>Encryption at host.</p> <p>Server-side encryption of Azure Disk Storage: Most Azure managed disks are encrypted with Azure Storage encryption, which uses server-side encryption (SSE) to protect your data and to help you meet your organizational security and compliance commitments. Azure Storage encryption automatically encrypts your data stored on Azure managed disks (OS and data disks) at rest by default when persisting it to the cloud. Disks with encryption at host enabled, however, are not encrypted through Azure Storage. For disks with encryption at host enabled, the server hosting your VM provides the encryption for your data, and that encrypted data flows into Azure Storage.</p> <p>Azure Disk Encryption: helps protect and safeguard your data to meet your organizational security and compliance commitments. ADE encrypts the OS and data disks of Azure virtual machines (VMs) inside your VMs by using the DM-Crypt feature of Linux or the BitLocker feature of Windows.</p> <p>Encryption at host - End-to-end encryption for your VM data: When you enable encryption at host, that encryption starts on the VM host itself, the Azure server that your VM is allocated to. The data for your temporary disk and OS/data disk caches are stored on that VM host. After enabling encryption at host, all this data is encrypted at rest and flows encrypted to the Storage service, where it is persisted. Essentially, encryption at host encrypts your data from end-to-end. Encryption at host does not use your VM's CPU and doesn't impact your VM's performance.</p> <p>Server-side encryption versus Azure disk encryption</p>

	<p>Azure Disk Encryption leverages either the DM-Crypt feature of Linux or the BitLocker feature of Windows to encrypt managed disks with customer-managed keys within the guest VM.</p> <p>Server-side encryption with customer-managed keys improves on ADE by enabling you to use any OS types and images for your VMs by encrypting data in the Storage service.</p>
Encryption key management	<p>Platform-managed keys</p> <p>By default, managed disks use platform-managed encryption keys. All managed disks, snapshots, images, and data written to existing managed disks are automatically encrypted-at-rest with platform-managed keys.</p> <p>Customer-managed keys</p> <p>You can choose to manage encryption at the level of each managed disk, with your own keys. When you specify a customer-managed key, that key is used to protect and control access to the key that encrypts your data. Customer-managed keys offer greater flexibility to manage access controls.</p> <p>Disk Encryption Sets</p>

SSE+CMK Workflow



1. An Azure Key Vault administrator creates key vault resources.
2. The key vault admin either imports their RSA keys to Key Vault or generate new RSA keys in Key Vault.
3. That administrator creates an instance of Disk Encryption Set resource, specifying an Azure Key Vault ID and a key URL. Disk Encryption Set is a new resource introduced for simplifying the key management for managed disks.
4. **When a disk encryption set is created, a [system-assigned managed identity](#) is created in Azure Active Directory (AD) and associated with the disk encryption set.**
5. The Azure key vault administrator then grants the managed identity permission to perform operations in the key vault.
6. A VM user creates disks by associating them with the disk encryption set. The VM user can also enable server-side encryption with customer-managed keys for existing resources by associating them with the disk encryption set.
7. Managed disks use the managed identity to send requests to the Azure Key Vault.

	<p>8. For reading or writing data, managed disks sends requests to Azure Key Vault to encrypt (wrap) and decrypt (unwrap) the data encryption key in order to perform encryption and decryption of the data.</p> <p>Double encryption at rest</p> <p>High security sensitive customers who are concerned of the risk associated with any particular encryption algorithm, implementation, or key being compromised can now opt for an additional layer of encryption using a different encryption algorithm/mode at the infrastructure layer using platform managed encryption keys. This new layer can be applied to persisted OS and data disks, snapshots, and images, all of which will be encrypted at rest with double encryption.</p>
<p>Backup and data protection</p>	
<p>How the backup and restore process works</p>	<ul style="list-style-type: none">• The first step in configuring backup for Azure Managed Disks is creating a Backup vault.• Then create a Backup policy that allows you to configure backup frequency and retention duration.• To configure backup, go to the Backup vault, assign a backup policy, select the managed disk that needs to be backed up and provide a resource group where the snapshots are to be stored and managed.• Once you configure the backup of a managed disk, a backup instance will be created within the backup vault. Using the backup instance, you can find health of backup operations, trigger on-demand backups, and perform restore operations.• Backup Vault uses Managed Identity to access other Azure resources. To configure backup of a managed disk and to restore from past backup, Backup Vault's managed identity requires a set of permissions on the source disk, the snapshot resource group where snapshots are created and managed, and the target resource group where you want to restore the backup.
<p>Security</p>	
<p>Azure Virtual Machines security overview</p>	<p>Antimalware</p> <p>Hardware security module</p> <p>Virtual machine disk encryption</p>

	<div>Virtual machine backup</div> <div>Azure Site Recovery</div> <div>Virtual networking</div> <div>Security policy management and reporting</div> <div>Compliance</div> <div>Confidential Computing</div>
What is Microsoft Defender for Cloud?	
Configure managed identities for Azure resources on a VM using the Azure portal	<div>Here are some of the benefits of using managed identities:</div> <div><ul style="list-style-type: none">You don't need to manage credentials. Credentials aren't even accessible to you.You can use managed identities to authenticate to any resource that supports Azure AD authentication, including your own applications.Managed identities can be used at no extra cost.</div> <div>There are two types of managed identities:</div> <div><ul style="list-style-type: none">System-assignedUser-assigned</div> <div>The following table shows the differences between the two types of managed identities:</div>

	<table><tr><th>Property</th><th>System-assigned managed identity</th><th>User-assigned managed identity</th></tr><tr><td>Creation</td><td>Created as part of an Azure resource (for example, Azure Virtual Machines or Azure App Service).</td><td>Created as a stand-alone Azure resource.</td></tr><tr><td>Life cycle</td><td>Shared life cycle with the Azure resource that the managed identity is created with. When the parent resource is deleted, the managed identity is deleted as well.</td><td>Independent life cycle. Must be explicitly deleted.</td></tr><tr><td>Sharing across Azure resources</td><td>Can't be shared. It can only be associated with a single Azure resource.</td><td>Can be shared. The same user-assigned managed identity can be associated with more than one Azure resource.</td></tr><tr><td>Common use cases</td><td>Workloads contained within a single Azure resource. Workloads needing independent identities. For example, an application that runs on a single virtual machine.</td><td>Workloads that run on multiple resources and can share a single identity. Workloads needing pre-authorization to a secure resource, as part of a provisioning flow. Workloads where resources are recycled frequently, but permissions should stay consistent. For example, a workload where multiple virtual machines need to access the same resource.</td></tr></table>	Property	System-assigned managed identity	User-assigned managed identity	Creation	Created as part of an Azure resource (for example, Azure Virtual Machines or Azure App Service).	Created as a stand-alone Azure resource.	Life cycle	Shared life cycle with the Azure resource that the managed identity is created with. When the parent resource is deleted, the managed identity is deleted as well.	Independent life cycle. Must be explicitly deleted.	Sharing across Azure resources	Can't be shared. It can only be associated with a single Azure resource.	Can be shared. The same user-assigned managed identity can be associated with more than one Azure resource.	Common use cases	Workloads contained within a single Azure resource. Workloads needing independent identities. For example, an application that runs on a single virtual machine.	Workloads that run on multiple resources and can share a single identity. Workloads needing pre-authorization to a secure resource, as part of a provisioning flow. Workloads where resources are recycled frequently, but permissions should stay consistent. For example, a workload where multiple virtual machines need to access the same resource.
Property	System-assigned managed identity	User-assigned managed identity														
Creation	Created as part of an Azure resource (for example, Azure Virtual Machines or Azure App Service).	Created as a stand-alone Azure resource.														
Life cycle	Shared life cycle with the Azure resource that the managed identity is created with. When the parent resource is deleted, the managed identity is deleted as well.	Independent life cycle. Must be explicitly deleted.														
Sharing across Azure resources	Can't be shared. It can only be associated with a single Azure resource.	Can be shared. The same user-assigned managed identity can be associated with more than one Azure resource.														
Common use cases	Workloads contained within a single Azure resource. Workloads needing independent identities. For example, an application that runs on a single virtual machine.	Workloads that run on multiple resources and can share a single identity. Workloads needing pre-authorization to a secure resource, as part of a provisioning flow. Workloads where resources are recycled frequently, but permissions should stay consistent. For example, a workload where multiple virtual machines need to access the same resource.														

Updates and maintenance overview

Automatic OS image upgrade	<p>Enabling automatic OS image upgrades on your scale set helps ease update management by safely and automatically upgrading the OS disk for all instances in the scale set.</p> <p>Automatic OS upgrade has the following characteristics:</p> <ul style="list-style-type: none">• Once configured, the latest OS image published by image publishers is automatically applied to the scale set without user intervention.• Upgrades batches of instances in a rolling manner each time a new image is published by the publisher.• Integrates with application health probes and Application Health extension.• You can opt out of automatic upgrades at any time (OS Upgrades can be initiated manually as well).• The OS Disk of a VM is replaced with the new OS Disk created with latest image version. Configured extensions and custom data scripts are run, while persisted data disks are retained.
----------------------------	---

	<ul style="list-style-type: none">• Extension sequencing is supported. <h2>Create a virtual machine scale set</h2> <div><div>Basics</div><div>Disks</div><div>Networking</div><div>Scaling</div><div>Management</div></div> <p>Configure monitoring and management options for your virtual machine scale set</p> <p>Microsoft Defender for Cloud</p> <p>Overprovisioning</p> <p>With overprovisioning turned on, the scale set actually spins up more VMs than you asked for. The requested number of VMs are successfully provisioned. Overprovisioning improves patch deployment time. You are not billed for the extra VMs, and they do not count toward your quota. Learn more about overprovisioning</p> <p>Enable overprovisioning <input type="checkbox"/></p> <p>Guest OS updates</p> <p>Enable automatic OS upgrades <input type="checkbox"/></p>
Automatic VM guest patching	<p>Enabling automatic VM guest patching for your Azure VMs helps ease update management by safely and automatically patching virtual machines to maintain security compliance.</p> <p>If automatic VM guest patching is enabled on a VM, then the available <i>Critical</i> and <i>Security</i> patches are downloaded and applied automatically on the VM. This process kicks off automatically every month when new patches are released. Patch assessment and installation are automatic, and the process includes rebooting the VM as required.</p> <h3>Patch orchestration modes</h3> <p>VMs on Azure now support the following patch orchestration modes:</p>

AutomaticByPlatform (Azure-orchestrated patching):

- This mode is supported for both Linux and Windows VMs.
- This mode enables automatic VM guest patching for the virtual machine and subsequent patch installation is orchestrated by Azure.
- This mode is required for availability-first patching.

AutomaticByOS:

- This mode is supported only for Windows VMs.
- This mode enables Automatic Updates on the Windows virtual machine, and patches are installed on the VM through Automatic Updates.
- This mode does not support availability-first patching.
- This mode is set by default if no other patch mode is specified for a Windows VM.

Manual:

- This mode is supported only for Windows VMs.
- This mode disables Automatic Updates on the Windows virtual machine. When deploying a VM using CLI or PowerShell, setting `--enable-auto-updates` to `false` will also set `patchMode` to `manual` and will disable Automatic Updates.

ImageDefault:

- This mode is supported only for Linux VMs.
- This mode does not support availability-first patching.
- This mode honors the default patching configuration in the image used to create the VM.

Azure portal

When creating a VM using the Azure portal, patch orchestration modes can be set under the Management tab for both Linux and Windows.

	<div> <div> <h3>Auto-shutdown</h3> <p>Enable auto-shutdown ^① <input checked="" type="checkbox"/></p> <p>Shutdown time ^① <input type="text" value="7:00:00 PM"/></p> <p>Time zone ^① <input type="text" value="UTC Coordinated Universal Time"/></p> <p>Notification before shutdown ^① <input type="text" value="Automatic by OS (Windows Automatic Updates)"/></p> <p>Email * ^① <input type="text" value=""/></p> </div> <div> <h3>Backup</h3> <p>Enable backup ^① <input type="checkbox"/></p> </div> <div> <h3>Guest OS updates</h3> <p>Patch orchestration options ^① <input type="text" value="Image default"/></p> <p>ⁱ Some patch orchestration options are not available for this image. Learn more</p> </div> </div> <div> <div>Review + create</div> <div>< Previous</div> <div>Next : Advanced ></div> </div>
Automatic extension upgrade	<p>When Automatic Extension Upgrade is enabled on a VM or scale set, the extension is upgraded automatically whenever the extension publisher releases a new version for that extension.</p> <h3>Azure CLI for Virtual Machines</h3>

	<div><div>Azure CLI</div><pre>az vm extension set \ --resource-group myResourceGroup \ --vm-name myVM \ --name DependencyAgentLinux \ --publisher Microsoft.Azure.Monitoring.DependencyAgent \ --version 9.5 \ --enable-auto-upgrade true</pre></div> <div>Azure CLI for Virtual Machine Scale Sets</div> <div><div>Azure CLI</div><pre>az vmss extension set \ --resource-group myResourceGroup \ --vmss-name myVMSS \ --name DependencyAgentLinux \ --publisher Microsoft.Azure.Monitoring.DependencyAgent \ --version 9.5 \ --enable-auto-upgrade true</pre></div>
Hotpatch	<p>Hotpatching is a new way to install updates on new Windows Server Azure Edition virtual machines (VMs) that doesn't require a reboot after installation.</p> <p>Understanding the patch status for your VM</p> <p>To view the patch status for your VM, navigate to the Guest + host updates section for your VM in the Azure portal. Under the Guest OS updates section, click on 'Go to Hotpatch (Preview)' to view the latest patch status for your VM.</p> <p>On this screen, you'll see the Hotpatch status for your VM. You can also review if there are any available patches for your VM that haven't been installed. As described in the 'Patch installation' section above, all security and critical updates will be automatically installed on your VM using Automatic VM Guest Patching and no extra actions are required.</p>

Azure update management	You can use Update Management in Azure Automation to manage operating system updates for your Windows and Linux virtual machines in Azure, in on-premises environments, and in other cloud environments. You can quickly assess the status of available updates on all agent machines and manage the process of installing required updates for servers.
Update management center	Update management center (preview) is a new-age unified service in Azure to manage and govern updates (Windows and Linux), both on-premises and other cloud platforms, across hybrid environments from a single dashboard. The new functionality provides native and out-of-the-box experience, granular access controls, flexibility to create schedules or take action now, ability to check updates automatically and much more.
Maintenance control	<p>Manage platform updates that don't require a reboot, using maintenance control. Azure frequently updates its infrastructure to improve reliability, performance, security or launch new features. Most updates are transparent to users. Some sensitive workloads, like gaming, media streaming, and financial transactions, can't tolerate even a few seconds of a VM freezing or disconnecting for maintenance. Maintenance control gives you the option to wait on platform updates and apply them within a 35-day rolling window.</p> <p>Maintenance control lets you decide when to apply updates to your isolated VMs and Azure dedicated hosts.</p>
Scheduled events	Scheduled Events is an Azure Metadata Service that gives your application time to prepare for virtual machine (VM) maintenance. It provides information about upcoming maintenance events (for example, reboot) so that your application can prepare for them and limit disruption. It's available for all Azure Virtual Machines types, including PaaS and IaaS on both Windows and Linux.
Monitor Azure virtual machines	
	<p>Azure Monitor is a full stack monitoring service that provides a complete set of features to monitor your Azure resources.</p> <p>To begin exploring Azure Monitor, go to the Overview page for your virtual machine, and then select the Monitoring tab. You can see the number of active alerts on the tab.</p>

vm

Virtual machine

Search

Overview

Activity log

Access control (IAM)

Tags

Diagnose and solve problems

Settings

Networking

Connect

Disks

Size

Microsoft Defender for Cloud

Advisor recommendations

Extensions + applications

Continuous delivery

Connect

Start

Restart

Stop

Capture

vm virtual machine agent status is not ready. Troubleshoot the issue

Availability zone : 1

Tags (edit) : [Click here to add tags](#)

Properties **Monitoring** Capabilities (7) Recommend:

Alerts

! Enable recommended alert rules

Get notified on important monitoring events by enabling commonly used alert rules or creating your own custom rules.

Enable

Create alert rule

Key Metrics

[See all metrics](#)

Show data for last:

1 hour

6 hours

The Key Metrics pane includes charts that show key health metrics, such as average CPU and network utilization

Activity log

The [Activity log](#) displays recent activity by the virtual machine, including any configuration changes and when it was stopped and started. View the Activity log in the Azure portal, or create a [diagnostic setting to send it to a Log Analytics workspace](#), where you can view events over time or analyze them with other collected data.

Collect guest metrics and logs	<p>Azure Monitor starts automatically collecting metric data for your virtual machine host when you create the VM. To collect metrics from the guest operating system of the virtual machine, though, you must install an agent. When you enable VM insights, the Log Analytics agent is installed and starts sending performance data to Azure Monitor Logs.</p>
Analyze logs	<p>Data in Azure Monitor Logs is stored in a Log Analytics workspace, where it's separated into tables, each with its own set of unique properties.</p> <p>VM insights store the collected data in logs, and the insights provide performance and map views that you can use to interactively analyze the data. You can work directly with this data to drill down further or perform custom analyses.</p>
Monitor Agents	<p>Azure Monitor Agent (AMA) collects monitoring data from the guest operating system of Azure and hybrid virtual machines and delivers it to Azure Monitor for use by features, insights, and other services.</p> <p>Limitations of the Log Analytics agent:</p> <ul style="list-style-type: none"> • Can't send data to Azure Monitor Metrics, Azure Storage, or Azure Event Hubs. • Difficult to configure unique monitoring definitions for individual agents. • Difficult to manage at scale because each virtual machine has a unique configuration.

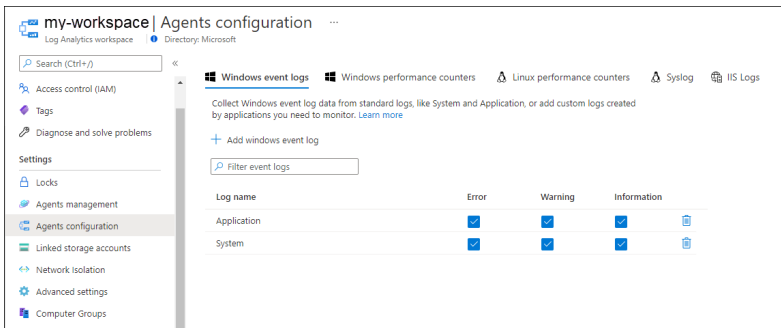
Windows agents

	Azure Monitor Agent	Log Analytics Agent	Diagnostics extension (WAD)
Environments supported			
Azure	X	X	X
Other cloud (Azure Arc)	X	X	
On-premises (Azure Arc)	X	X	
Windows Client OS	X		
Data collected			
Event Logs	X	X	X
Performance	X	X	X
File based logs	X (Public preview)	X	X
IIS logs	X (Public preview)	X	X
ETW events			X
.NET app logs			X
Crash dumps			X
Agent diagnostics logs			X
Data sent to			
Azure Monitor Logs	X	X	
Azure Monitor Metrics ¹	X		X
Azure Storage			X
Event Hub			X
Services and features supported			
Microsoft Sentinel	X (View scope)	X	
VM Insights	X (Public preview)	X	
Microsoft Defender for Cloud	X (Public preview)	X	
Update Management	X (Public preview, independent of monitoring agents)	X	
Change Tracking		X	

Configure data sources

To configure data sources for Log Analytics agents, go to the Log Analytics workspaces menu in the Azure portal and select a workspace. Select Agents configuration.

Any configuration is delivered to all agents connected to that workspace. You can't exclude any connected agents from this configuration.



Overview of VM insights

VM insights monitors the performance and health of your virtual machines and virtual machine scale sets. It monitors their running processes and dependencies on other resources.

VM insights stores its data in Azure Monitor Logs, which allows it to deliver powerful aggregation and filtering and to analyze data trends over time. You can view this data in a single VM from the virtual machine directly.

Map experience:

The Map feature visualizes the VM dependencies by discovering running processes that have:

- Active network connections between servers.
- Inbound and outbound connection latency.
- Ports across any TCP-connected architecture over a specified time range.

Azure boot diagnostics

Boot diagnostics is a debugging feature for Azure virtual machines (VM) that allows diagnosis of VM boot failures. Boot diagnostics enables a user to observe the state of their VM as it is booting up by collecting serial log information and screenshots.

When you create a VM in Azure portal, boot diagnostics is enabled by default. The recommended boot diagnostics experience is to use a managed storage account, as it yields significant performance improvements in the time to create an Azure VM.

An alternative boot diagnostic experience is to use a custom storage account.

Create a virtual machine

Basics Disks Networking Management Advanced Tags Review + create

Configure monitoring and management options for your VM.

Azure Security Center
Azure Security Center provides unified security management and advanced threat protection across hybrid cloud workloads.
[Learn more](#)

✔ Your subscription is protected by Azure Security Center basic plan.

Monitoring

Enable detailed monitoring ⓘ ☐ On ☒ Off


Boot diagnostics ⓘ ☒ Enable with managed storage account (recommended)

☐ Enable with custom storage account

☐ Disable

OS guest diagnostics ⓘ ☐ On ☒ Off

Boot diagnostics view: Go to the virtual machine blade in the Azure portal, the boot diagnostics option is under the *Support and Troubleshooting* section in the Azure portal. Selecting boot diagnostics will display a screenshot and serial log information. The serial log contains kernel messaging and the screenshot is a snapshot of your VMs current state.

	<div><div><div>contosold-windows Boot diagnostics</div><div>Virtual machine</div><div><div>Search (Ctrl+F)</div><div>Refresh</div><div>Settings</div></div><div><div>Run command</div><div>Monitoring</div><div>Insights</div><div>Alerts</div><div>Metrics</div><div>Diagnostics settings</div><div>Logs</div><div>Connection monitor</div><div>Support + troubleshooting</div><div>Resource health</div><div>Boot diagnostics</div><div>Performance diagnostics (Prev...</div><div>Reset password</div><div>Redeploy</div><div>Maintenance</div><div>Serial console</div><div>Connection troubleshoot</div><div>New support request</div></div></div><div><div>ScreenshotSerial log</div><div>Updated: Thursday, August 6, 2020, 5:55:36 PM UTCDownload screenshot</div><div><div><div>Press Ctrl+Alt+Delete to unlock.</div><div>5:55</div><div>Thursday, August 6</div></div></div></div></div>
--	---

Backup and Recovery

Backup and restore options for virtual machines in Azure	<div><div><h3>Azure Backup</h3><p>You'll use Azure Backup for most use-cases involving backup operations on Azure VMs running production workloads. Azure Backup supports application-consistent backups for both Windows and Linux VMs. Azure Backup creates recovery points that are stored in geo-redundant recovery vaults. When you restore from a recovery point, you can restore the entire VM or specific files.</p></div><div><h3>Azure Site Recovery</h3><p>Azure Site Recovery protects your VMs from a major disaster scenario. These scenarios may include widespread service interruptions or regional outages caused by natural disasters. You can configure Azure Site Recovery for your VMs so that your</p></div></div>
--	---

	<p>applications are recoverable in a matter of minutes with a single click. You can replicate to an Azure region of your choice, since recovery isn't restricted to paired regions.</p> <h2>Managed snapshots</h2> <p>In development and test environments, snapshots provide a quick and simple option for backing up VMs that use managed disks. A managed snapshot is a full, read-only copy of a managed disk. Snapshots exist independently of their source disks.</p>
Azure VM backup	<p>Azure Backup provides independent and isolated backups to guard against unintended destruction of the data on your VMs. Backups are stored in a Recovery Services vault with built-in management of recovery points. Configuration and scaling are simple, backups are optimized, and you can easily restore as needed.</p> <p>Backup process:</p> <p>Here's how Azure Backup completes a backup for Azure VMs:</p> <ol style="list-style-type: none">1. For Azure VMs that are selected for backup, Azure Backup starts a backup job according to the backup schedule you specify.2. During the first backup, a backup extension is installed on the VM if the VM is running.<ul style="list-style-type: none">○ For Windows VMs, the VMSnapshot extension is installed.○ For Linux VMs, the VMSnapshotLinux extension is installed.3. For Windows VMs that are running, Backup coordinates with Windows Volume Shadow Copy Service (VSS) to take an app-consistent snapshot of the VM.<ul style="list-style-type: none">○ By default, Backup takes full VSS backups.○ If Backup can't take an app-consistent snapshot, then it takes a file-consistent snapshot of the underlying storage (because no application writes occur while the VM is stopped).4. For Linux VMs, Backup takes a file-consistent backup. For app-consistent snapshots, you need to manually customize pre/post scripts.5. After Backup takes the snapshot, it transfers the data to the vault.

Snapshot consistency	<table><tr><th>Snapshot</th><th>Details</th><th>Recovery</th><th>Consideration</th></tr><tr><td>Application-consistent</td><td>App-consistent backups capture memory content and pending I/O operations. App-consistent snapshots use a VSS writer (or pre/post scripts for Linux) to ensure the consistency of the app data before a backup occurs.</td><td>When you're recovering a VM with an app-consistent snapshot, the VM boots up. There's no data corruption or loss. The apps start in a consistent state.</td><td>Windows: All VSS writers succeeded Linux: Pre/post scripts are configured and succeeded</td></tr><tr><td>File-system consistent</td><td>File-system consistent backups provide consistency by taking a snapshot of all files at the same time.</td><td>When you're recovering a VM with a file-system consistent snapshot, the VM boots up. There's no data corruption or loss. Apps need to implement their own "fix-up" mechanism to make sure that restored data is consistent.</td><td>Windows: Some VSS writers failed Linux: Default (if pre/post scripts aren't configured or failed)</td></tr><tr><td>Crash-consistent</td><td>Crash-consistent snapshots typically occur if an Azure VM shuts down at the time of backup. Only the data that already exists on the disk at the time of backup is captured and backed up.</td><td>Starts with the VM boot process followed by a disk check to fix corruption errors. Any in-memory data or write operations that weren't transferred to disk before the crash are lost. Apps implement their own data verification. For example, a database app can use its transaction log for verification. If the transaction log has entries that aren't in the database, the database software rolls transactions back until the data is consistent.</td><td>VM is in shutdown (stopped/deallocated) state.</td></tr></table>	Snapshot	Details	Recovery	Consideration	Application-consistent	App-consistent backups capture memory content and pending I/O operations. App-consistent snapshots use a VSS writer (or pre/post scripts for Linux) to ensure the consistency of the app data before a backup occurs.	When you're recovering a VM with an app-consistent snapshot, the VM boots up. There's no data corruption or loss. The apps start in a consistent state.	Windows: All VSS writers succeeded Linux: Pre/post scripts are configured and succeeded	File-system consistent	File-system consistent backups provide consistency by taking a snapshot of all files at the same time.	When you're recovering a VM with a file-system consistent snapshot, the VM boots up. There's no data corruption or loss. Apps need to implement their own "fix-up" mechanism to make sure that restored data is consistent.	Windows: Some VSS writers failed Linux: Default (if pre/post scripts aren't configured or failed)	Crash-consistent	Crash-consistent snapshots typically occur if an Azure VM shuts down at the time of backup. Only the data that already exists on the disk at the time of backup is captured and backed up.	Starts with the VM boot process followed by a disk check to fix corruption errors. Any in-memory data or write operations that weren't transferred to disk before the crash are lost. Apps implement their own data verification. For example, a database app can use its transaction log for verification. If the transaction log has entries that aren't in the database, the database software rolls transactions back until the data is consistent.	VM is in shutdown (stopped/deallocated) state.
Snapshot	Details	Recovery	Consideration														
Application-consistent	App-consistent backups capture memory content and pending I/O operations. App-consistent snapshots use a VSS writer (or pre/post scripts for Linux) to ensure the consistency of the app data before a backup occurs.	When you're recovering a VM with an app-consistent snapshot, the VM boots up. There's no data corruption or loss. The apps start in a consistent state.	Windows: All VSS writers succeeded Linux: Pre/post scripts are configured and succeeded														
File-system consistent	File-system consistent backups provide consistency by taking a snapshot of all files at the same time.	When you're recovering a VM with a file-system consistent snapshot, the VM boots up. There's no data corruption or loss. Apps need to implement their own "fix-up" mechanism to make sure that restored data is consistent.	Windows: Some VSS writers failed Linux: Default (if pre/post scripts aren't configured or failed)														
Crash-consistent	Crash-consistent snapshots typically occur if an Azure VM shuts down at the time of backup. Only the data that already exists on the disk at the time of backup is captured and backed up.	Starts with the VM boot process followed by a disk check to fix corruption errors. Any in-memory data or write operations that weren't transferred to disk before the crash are lost. Apps implement their own data verification. For example, a database app can use its transaction log for verification. If the transaction log has entries that aren't in the database, the database software rolls transactions back until the data is consistent.	VM is in shutdown (stopped/deallocated) state.														
Use infrastructure automation tools with virtual machines in Azure	<ul style="list-style-type: none">• Ansible• Chef• Puppet• Cloud-init• PowerShell DSC• Azure Custom Script Extension• Packer• Terraform• Azure Automation: Azure Automation uses runbooks to process a set of tasks on the VMs you target. Azure Automation is used to manage existing VMs rather than to create an infrastructure. Azure Automation can run across both Linux and Windows VMs, as well as on-premises virtual or physical machines with a hybrid runbook worker. Runbooks can be stored in a source control repository, such as GitHub. These runbooks can then run manually or on a defined schedule. Azure Automation also provides a Desired State Configuration (DSC) service that allows you to create definitions for how a given set of VMs should be configured. DSC then ensures that the required configuration is applied and the VM stays consistent. Azure Automation DSC runs on both																

	<div>Windows and Linux machines.</div> <ul style="list-style-type: none">• Azure DevOps Services• Jenkins• Azure Resource Manager template
<h2>User Data for Azure Virtual Machine</h2>	
What is "user data"	<p>User data is a set of scripts or other metadata, that will be inserted to an Azure virtual machine at provision time. Any application on the virtual machine can access the user data from the Azure Instance Metadata Service (IMDS) after provision.</p> <p>User data is a new version of custom data and it offers added benefits:</p> <ul style="list-style-type: none">• User data can be retrieved from Azure Instance Metadata Service(IMDS) after provision.• User data is persistent. It will be available during the lifetime of the VM.• User data can be updated from outside the VM, without stopping or rebooting the VM.• User data can be queried via GET VM/VMSS API with \$expand option.• In addition, if user data is not added at provision time, you can still add it after provision.
	<h3>Retrieving user data</h3> <p>Single VMs:</p> <pre>GET "/subscriptions/{guid}/resourceGroups/{RGName}/providers/Microsoft.Compute/virtualMachines/{VMName}?\$expand=userData"</pre> <p>Virtual machine scale set:</p> <pre>GET "/subscriptions/{guid}/resourceGroups/{RGName}/providers/Microsoft.Compute/virtualMachineScaleSets/{VMSSName}?\$expand=userData"</pre> <p>Virtual machine scale set VM:</p> <pre>GET "/subscriptions/{guid}/resourceGroups/{RGName}/providers/Microsoft.Compute/virtualMachineScaleSets/{VMSSName}/virtualMachines/{vmss instance id}?\$expand=userData"</pre>

	<div><div>Updating user data</div><div>With REST API, you can use a normal PUT or PATCH request to update the user data. The user data will be updated without the need to stop or reboot the VM.</div><div>PUT "/subscriptions/{guid}/resourceGroups/{RGName}/providers/Microsoft.Compute/ virtualMachines/{VMName}</div><div>PATCH "/subscriptions/{guid}/resourceGroups/{RGName}/providers/Microsoft.Compute/ virtualMachines/{VMName}</div></div>
Custom data and cloud-init on Azure Virtual Machines	<div><div>You might need to inject a script or other metadata into a Microsoft Azure virtual machine (VM) at provisioning time. In other clouds, this concept is often called <i>user data</i>. Microsoft Azure has a similar feature called <i>custom data</i>.</div><div>Custom data is made available to the VM during first startup or setup, which is called <i>provisioning</i>. Provisioning is the process where VM creation parameters (for example, host name, username, password, certificates, custom data, and keys) are made available to the VM. A provisioning agent, such as the Linux Agent or cloud-init, processes those parameters.</div><div>Pass custom data to the VM</div><div><div>Azure CLI</div><pre>az vm create \ --resource-group myResourceGroup \ --name centos74 \ --image OpenLogic:CentOS-CI:7-CI:latest \ --custom-data cloud-init.txt \ --generate-ssh-keys</pre></div></div>

